HIRSCHMANN
A BELDEN BRAND

Reference Manual

Web-based Interface
Industrial ETHERNET (Gigabit) Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS

Technical Support
HAC-Support@hirschmann.de

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2009 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann gives no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann accepts no responsibility for any damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can find the current version of this manual on the Internet, on the Hirschmann product pages (www.hirschmann-ac.de).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Content

Content 3

About this Manual 7

Key 9

Opening the Web-based Interface 11

1 Basic Settings 15

1.1 System 16

1.2 Network 21

1.3 Software 23
1.3.1 View the software versions present on the device 23
1.3.2 Update via file selection 24
1.3.3 tftp update 24

1.4 Port configuration 25

1.5 Power over ETHERNET 27

1.6 Load/Save 29
1.6.1 Loading the configuration 30
1.6.2 Saving the configuration 30
1.6.3 URL 31
1.6.4 Deleting a configuration 31
1.6.5 Using the AutoConfiguration Adapter (ACA) 32
1.6.6 Canceling a configuration change 33

1.7 Restart 35

2 Security 37

2.1 Password / SNMP Access 38

2.2 SNMPv1/v2 Access Settings 40

2.3 Telnet/Web Access 43
2.3.1 Description of Telnet access 43
2.3.2 Description of Web access 44

2.4 Port Security 45

3 Time 49

3.1 SNTP configuration 51

3.2 PTP (IEEE 1588) 54
3.2.1 PTP Global (MS20/MS30, PowerMICE) 55
3.2.2 PTP Version 1 (MS20/MS30, Power MICE) 57
3.2.3 PTP Version 2 (BC) (MS20/MS30, PowerMICE) 60
3.2.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE) 65

4 Switching 69

4.1 Switching Global 70

4.2 Filters for MAC addresses 71

4.3 Rate Limiter 73
4.3.1 Rate Limiter settings 73

4.4 Multicasts 75
4.4.1 Global Configuration 75
4.4.2 IGMP Querier and IGMP settings 76
4.4.3 Unknown Multicasts 78
4.4.4 Known Multicasts 79
4.4.5 Settings per port (table) 80

4.5 VLAN 83
4.5.1 VLAN Global 83
4.5.2 Current VLAN 86
4.5.3 VLAN Static 88
4.5.4 VLAN Port 90

5 QoS/Priority 93

5.1 Global 94

5.2 Port configuration 97
5.2.1 Entering the port priority 98

5.3 802.1D/p Mapping 99

5.4 IP DSCP mapping 101

6 Redundancy 103

6.1 Ring Redundancy 104
6.1.1 Configuring the HIPER-Ring 106
6.1.2 Configuring the MRP-Ring 109

6.2 Ring/Network coupling 112
6.2.1 Preparing a Ring/Network coupling 112

6.3 Rapid Spanning Tree 119
6.3.1 Rapid Spanning Tree Global 121
6.3.2 Rapid Spanning Tree Port 125

7 Diagnosis 129

7.1 Event log 130

7.2 Ports 131
7.2.1 Statistics table 131
7.2.2 Utilization 132
7.2.3 SFP modules 133

7.3 Topology Discovery 134

7.4 Port Mirroring 136

7.5 Device Status 138

7.6 Signal contact 140
7.6.1 Manual setting 140
7.6.2 Function monitoring 140
7.6.3 Device status 142
7.6.4 Configuring traps 142

7.7 Alarms (Traps) 143

7.8 Report 145

7.9 IP address conflict detection 146

7.10 Self Test 148

7.11 Service mode 149
7.11.1 Activating the service mode 149
7.11.2 Deactivating the service mode 151

8 Advanced 153

8.1 DHCP Relay Agent 154

8.2 Industrial Protocols 156
8.2.1 PROFINET IO 157
8.2.2 EtherNet/IP 157

8.3 Command Line 158

A Appendix 159

A.1 Technical Data 160

A.2 List of RFCs 161

A.3 Based specifications and standards 163

A.4 Copyright of integrated software 164
A.4.1 Bouncy Castle Crypto APIs (Java) 164
A.4.2 LVL7 Systems, Inc. 165

B Readers' comments 167

C Index 169

D Further support 171

About this Manual

The "Web-based Interface" reference manual contains detailed information on using the Web interface to operate the individual functions of the device.

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and all the other information that you need to install the device before you begin with the configuration of the device.

The “Basic Configuration” user manual contains all the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Redundancy Configuration” user manual contains all the information you need to select a suitable redundancy procedure and configure it.

The “Industry Protocols” user manual describes how the device is connected by means of a communication protocol commonly used in the industry, such as EtherNet/IP and PROFINET.

The Network Management Software HiVision/Industrial HiVision provides you with additional options for smooth configuration and monitoring:

- Configuration of multiple devices simultaneously.
- Graphical interface with network layouts.
- Auto-topology discovery.
- Event log.
- Event handling.
- Client / Server structure.
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway

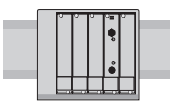
Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
■	Subheading
Link	Indicates a cross-reference with a stored link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

Symbols used:

	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge
	Hub

	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

Opening the Web-based Interface

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 1 or later, or Microsoft Internet Explorer version 6 or later.

Note: The Web-based interface uses the Java software version 5 or later (Java™ Runtime Environment Version 1.5.x or 6.x). If it is not installed on your computer yet, it will be installed automatically via the Internet when you start the Web-based interface for the first time.

For Windows users: If you don´t have any access to the internet cancel the installation. Install the software from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

Device Software
Device Info
AddOn Software
AddOn Info
Imprint
Exit
Java Runtime Environment 5
The Web-based interface uses the " Java™ Runtime Environment" plug-in. The Web-based interface of this device has been tested with the version of the plug-in on this CD-ROM.
JAVA™ 2 PLATFORM STANDARD EDITION
haneWIN DHCP-Server 2.0.29
Adobe Acrobat Reader
Java Runtime Environment 5
Instal
Website

Figure 1: Installing Java

☐ Start your Web browser.
☐ Make sure that you have activated JavaScript and Java in the security settings of your browser.

☐ Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:
`http://xxx.xxx.xxx.xxx`

The login window appears on the screen.

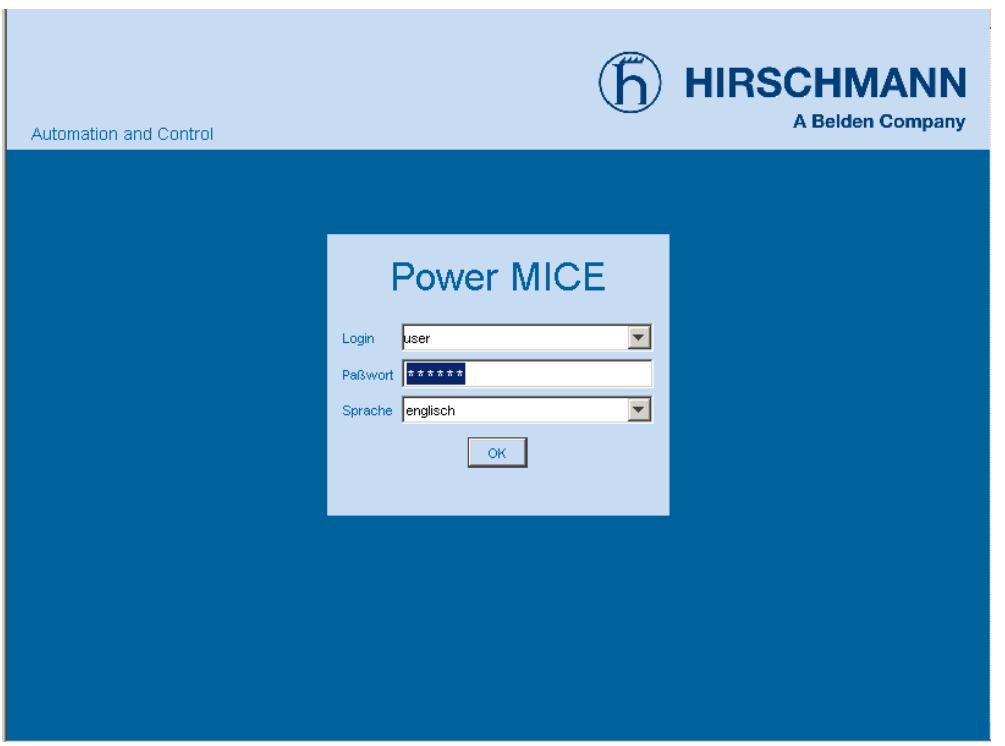


Figure 2: Login window

☐ Select the desired language.
☐ In the drop-down menu, you select
– user, to have read access, or
– admin, to have read and write access
to the device.
☐ The password “public”, with which you have read access, appears in the password field. If you wish to have write access to the device, then highlight the contents of the password field and overwrite it with the password “private” (default setting).
☐ Click on OK.

The Web site of the device appears on the screen.

Note: The changes you make in the dialogs are copied to the device when you click on “Set”. Click on “Load” to update the display.

Note: You can block your access to the device by entering an incorrect configuration.
Activating the function “Cancel configuration change” in the “Load/Save” dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.

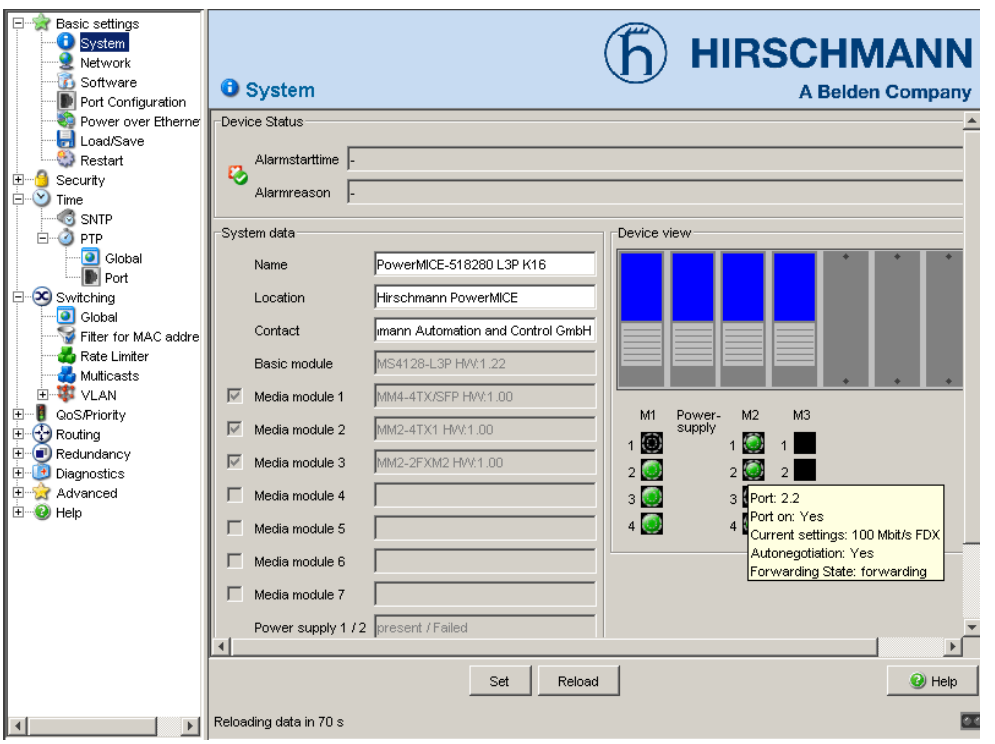
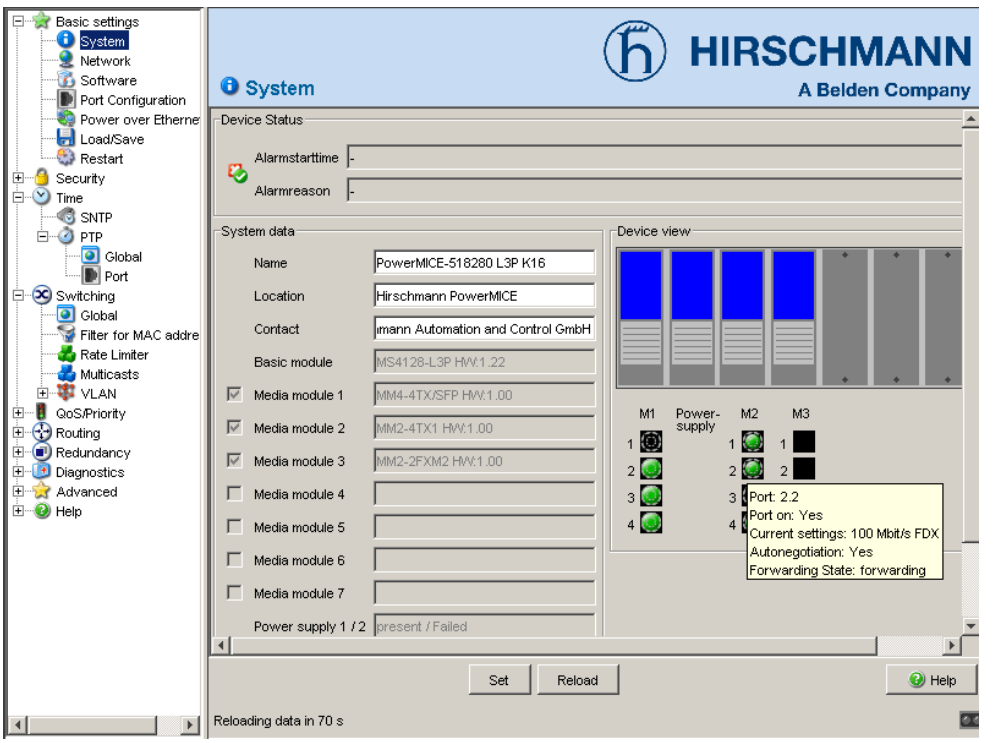


Figure 3: Website of the device with speech-bubble help

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the right mouse button you can use “Back” to return to a menu item you have already selected, or “Forward” to jump to a menu item you have already selected.



1 Basic Settings

The basic settings menu contains the dialogs, displays and tables for basic settings configuration:

- System
- Network
- Software
- Port configuration
- Power over Ethernet
- Load/Save
- Restart

1.1 System

The „System“ submenu in the basic settings menu is structured as follows:

- Device status
- System data
- Device view
- Reloading data

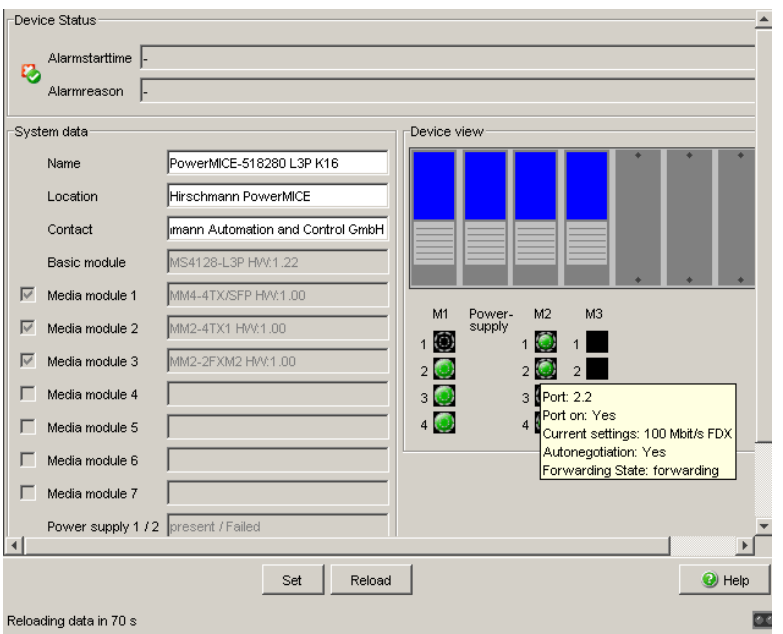


Figure 4: "System" submenu

Device status

This section of the website provides information on the device status and the alarm state of the device.

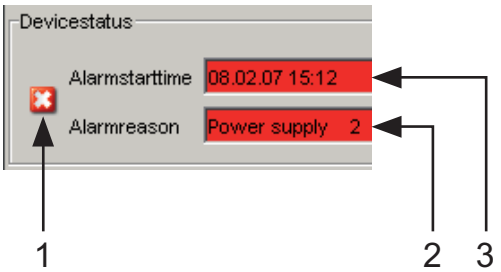


Figure 5: Device status and alarm display
1 - Symbol indicates the Device Status
2 - Cause of the oldest existing alarm
3 - Time of the oldest existing alarm

System data

This area of the website displays the system parameters of the device. Here you can change,

- the system name,
- the location description,
- the name of the contact person for this device,
- the availability of the media modules (see fig. 6) and
- the temperature threshold values.

Name	Meaning
Name	System name of this device
Location	Location of this device
Contact person	Contact person for this device
Basic module	Hardware version of the basic module
Media module 1	Hardware version of media module 1
Media module 2	Hardware version of media module 2
Media module 3	Hardware version of media module 3
Media module 4	Hardware version of media module 4
Media module 5	Hardware version of media module5
Media module 6	Hardware version of media module 6
Media module 7	Hardware version of media module 7
Power supply (P1/P2)	Status of the power supply units
Operating time	Time that has elapsed since the device was last restarted.
Temperature	Temperature in the device. Lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm message.

Table 1: System data

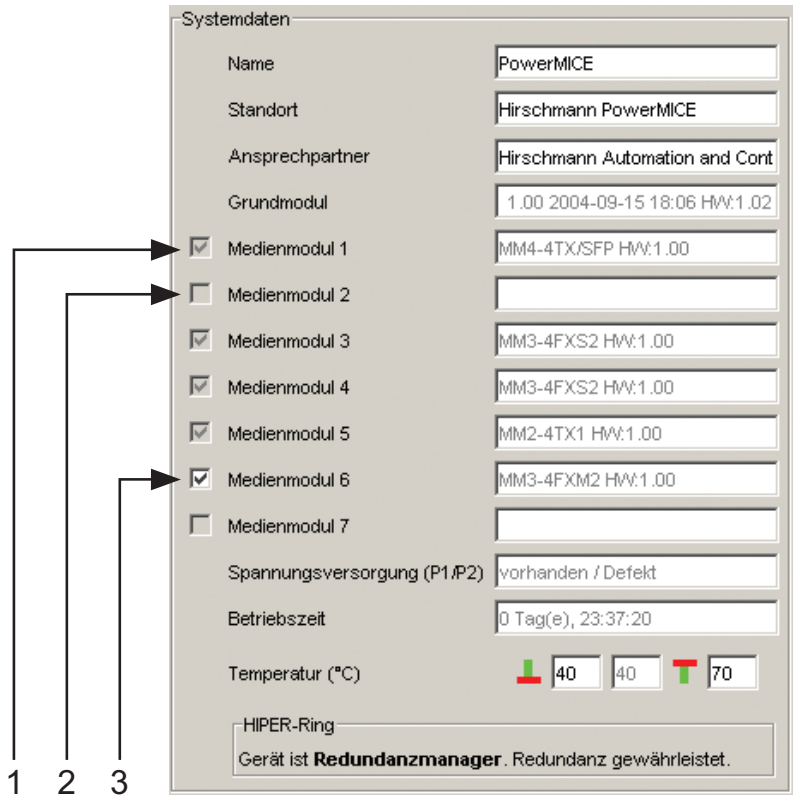


Figure 6: Availability of the media modules
1 - Module present
2 - Empty slot
3 - Module was removed. Click this check mark to define this slot as an empty slot.

Device view

The device view shows the device with the current configuration. The symbols underneath the device view represent the status of the individual ports.

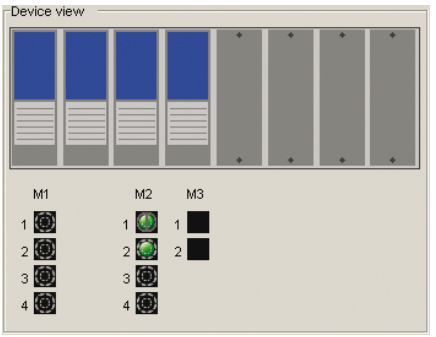


Figure 7: Device view

Meaning of the symbols:

The port (10, 100 Mbit/s, 1, 10 Gbit/s) is enabled and the connection is OK.

The port is disabled by the management and it has a connection.

The port is disabled by the management and it has no connection.

The port is in autonegotiation mode.

The port is in HDX mode.

The port is in RSTP discarding mode (100 Mbit/s).

The port is in routing mode (100 Mbit/s).

Updating

This area of the website at the bottom left displays the countdown time until the applet requests the current data of this dialog again. Clicking the "Update" button calls the current dialog information immediately.
The applet polls the current data of the device automatically every 100 seconds.

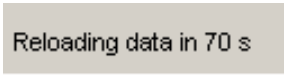


Figure 8: Time until update

1.2 Network

With the `Basic Settings:Network` dialog you define the source from which the device gets its IP parameters after starting, and you assign the IP parameters and VLAN ID and configure the HiDiscovery access.

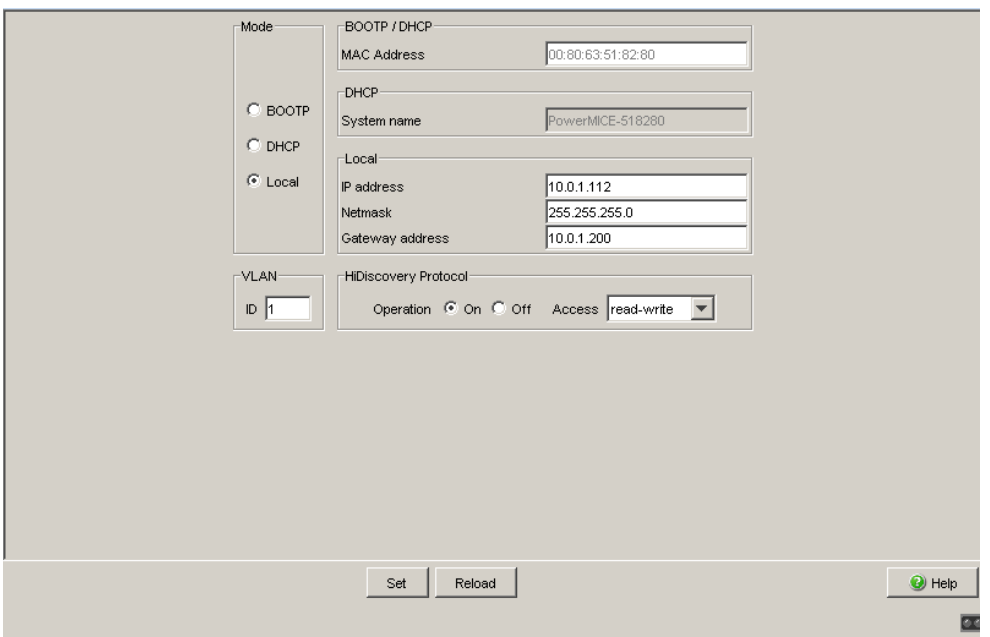


Figure 9: Network parameters dialog

☐ Under “Mode”, you enter where the device gets its IP parameters:
- In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see on page 30 „Saving the configuration“).
- In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device (see on page 30 „Saving the configuration“).
- In the local mode the net parameters in the device memory are used.

☐ Enter the parameters on the right according to the selected mode.

- ☐ You enter the name applicable to the DHCP protocol in the “Name” line in the system dialog of the Web-based interface.

- ☐ The “VLAN ID” frame enables you to assign a VLAN to the agent. If you enter the VLAN ID “0” here (not contained in the standard), the agent can be accessed from all VLANs.
- ☐ The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (setting on delivery: operation “on”, access “read-write”).

  The Ethernet Switch Configurator protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the Ethernet Switch Configurator Protocol if you want to allocate an IP address to the device from your PC with the enclosed Ethernet Switch Configurator protocol software (setting on delivery: operation “on”, access “read-write”).

1.3 Software

The software dialog enables you to view the software versions present on the device and to carry out a software update of the device via tftp or file selection.

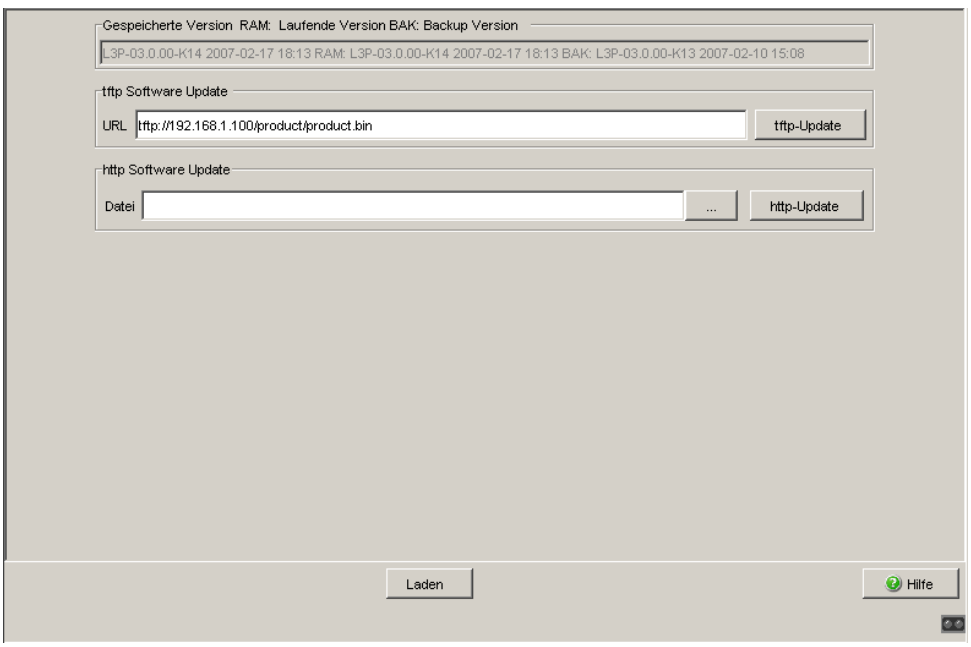


Figure 10: Software dialog

1.3.1 View the software versions present on the device

You can view:

- The software version stored in the flash memory (Stored Version).
- The currently loaded software version (RAM: Running Version).
- The previous software version stored in the flash memory (BAK: Backup Version).

1.3.2 Update via file selection

For an update via a file selection window, the device software must be on a data carrier that you can access via your PC.

☐ In the file selection frame, click on “...”.
☐ In the file selection window, select the device software (device.bin) and click on “Open”.
☐ Click on “Update” to transfer the software to the device.

The end of the update is indicated by one of the following messages:

- Update completed successfully.
- Update failed. Reason: incorrect file.
- Update failed. Reason: error when saving.
- File not found (reason: file name not found or does not exist).
- Connection error (reason: path without file name).

☐ After successfully loading it, you activate the new software:
Select the `Basic Settings:Restart` dialog and perform a cold start.
In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
☐ In your browser, click on “Reload” so that you can access the device again after it is booted.

1.3.3 tftp update

For a tftp update you need a tftp server on which the software to be loaded is stored.
The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://192.168.1.100/product/product.bin`).
Click "tftp Update" to load the software from the tftp server to the device.
To start the new software after loading, cold start the device (see on page 35 „Restart“).

1.4 Port configuration

This configuration table allows you to configure every port of the device.

- In the “Name” column, you can enter a name for every port.
- In the “Ports on” column, you can switch on the port by selecting it here.
- In the “Propagate connection error” column, you can specify that a link alarm will be forwarded to the device status and/or the the signal contact is to be opened.
- In the “Automatic Configuration” column, you can activate the automatic selection of the the operating mode (Autonegotiation) and the automatic assigning of the connections (Auto cable crossing) of a TP port by selecting the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
- In the “Manual Configuration” column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  - 10 Mbit/s half duplex (HDX),
  - 10 Mbit/s full duplex (FDX),
  - 100 Mbit/s half duplex (HDX),
  - 100 Mbit/s full duplex (FDX),
  - 1000 Mbit/s half duplex (HDX) and
  - 1000 Mbit/s full duplex (FDX).
- The “Link/Current operating mode” column displays the current operating mode and thereby also an existing connection.
- In the “Cable Crossing (Auto. Conf. off)” column, you assign the connections of a TP port, if “Automatic Configuration” is deactivated for this port. The possible settings are:
  - enable: the device swaps the send and receive line pairs of the TP cable for this port (MDIX).
  - disable: the device does not swap the send and receive line pairs of the TP cable for this port (MDI).
  - unsupported: the port does not support this function (optical port, TP SFP port).
- In the “Flow Control” column, you checkmark this port to specify that flow control is active here. You also activate the global “Flow Control” switch (see on page 70 „Switching Global“).

Note: If you have set up VLANs, pay attention to the “Transparent mode” (see on page 83 „VLAN Global“).

Note: The active automatic configuration has priority over the manual configuration.

Note: The following settings are required for the ring ports in a HIPER-Ring:

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	Off	On
Port	On	On
Duplex	Full	–

Table 2: Port settings for ring ports

When you switch the DIP switch for the ring ports, the device sets the required settings for the ring ports in the configuration table. The port, which has been switched from a ring port to a normal port, is given the settings Autonegotiation (automatic configuration) on and Port on. The settings remain changeable for all ports.

Figure 11: Port Configuration Table dialog

1.5 Power over ETHERNET

Devices with Power over ETHERNET (PoE) media modules or PoE ports enable you to supply current to terminal devices such as IP phones via the twisted-pair cable. PoE media modules and PoE ports support Power over ETHERNET according to IEEE 802.3af.
On delivery, the Power over ETHERNET function is activated globally and at all ports.
If the device is equipped with PoE media modules, you will then have the option of supplying current to devices such as IP phones via the twisted-pair cable. PoE media modules support Power over ETHERNET according to IEEE 802.3af.
On delivery, the Power over ETHERNET function is activated globally and on all ports.

Nominal power for MS20/30, MACH 1000 and Power MICE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 60 Watt per PoE media module for now.

Nominal power for OCTOPUS 8M-PoE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the device gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 15 Watt per PoE port for now.

- ☐ With “Function on/off” you turn the PoE on or off.
- ☐ With “Send Trap” you can get the device to send a trap in the following cases:
  - – If a value exceeds/falls below the performance threshold.
  - – If the PoE supply voltage is switched on/off at at least one port.
- ☐ Enter the power threshold in “Threshold”. When this value is exceeded/ not achieved, the device will send a trap, provided that “Send trap” is enabled. For the power threshold you enter the power yielded as a percentage of the nominal power.
- ☐ “Nominal Power” displays the power that the device nominally provides for all PoE ports together.

- ☐ “Reserved Power” displays the maximum power that the device provides to all the connected PoE devices together on the basis of their classification.
- ☐ “Delivered Power” shows how large the current power requirement is at all PoE ports.

The difference between the "nominal" and "reserved" power indicates how much power is still available to the free PoE ports.

- ☐ In the “POE on” column, you can enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ In the “Priority” column (MACH 4000), set the PoE priority of the port to “low”, “high” or “critical”.
- ☐ The “Class” column shows the class of the connected device:
  ClassMaximum power delivered
  0: 15.4 W = state on delivery
  1: 4.0 W
  2: 7.0 W
  3: 15,4 W
  4: reserved, treat as class 0
- ☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

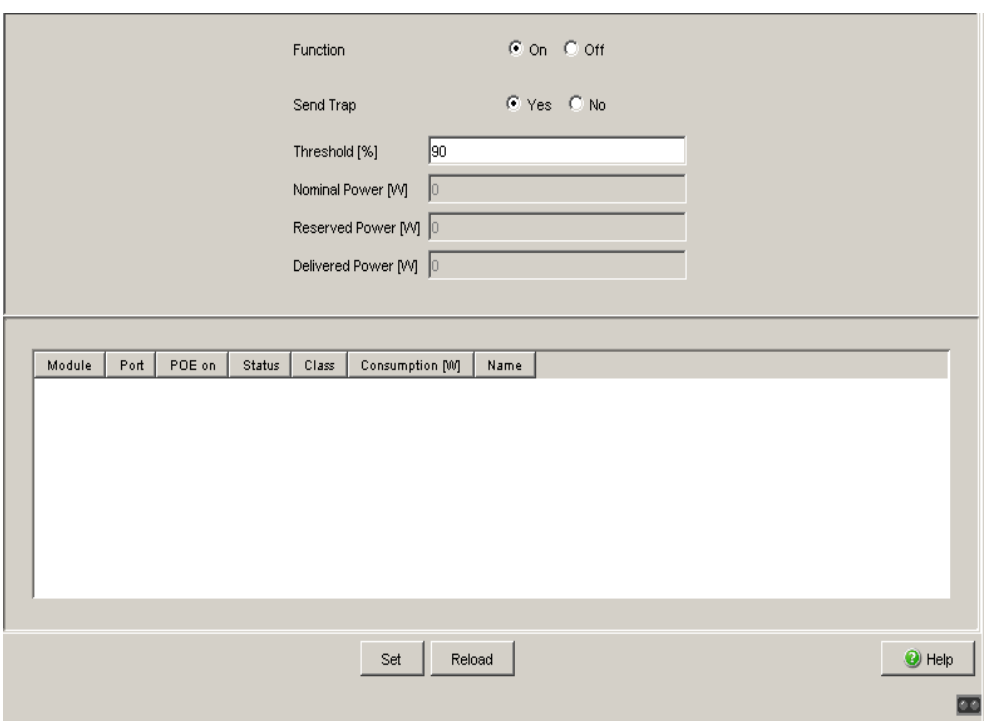


Figure 12: Power over Ethernet dialog

1.6 Load/Save

With this dialog you can:

- load a configuration,
- save a configuration,
- enter a URL,
- restore the delivery configuration,
- use the ACA for configuring,
- cancel a configuration change.

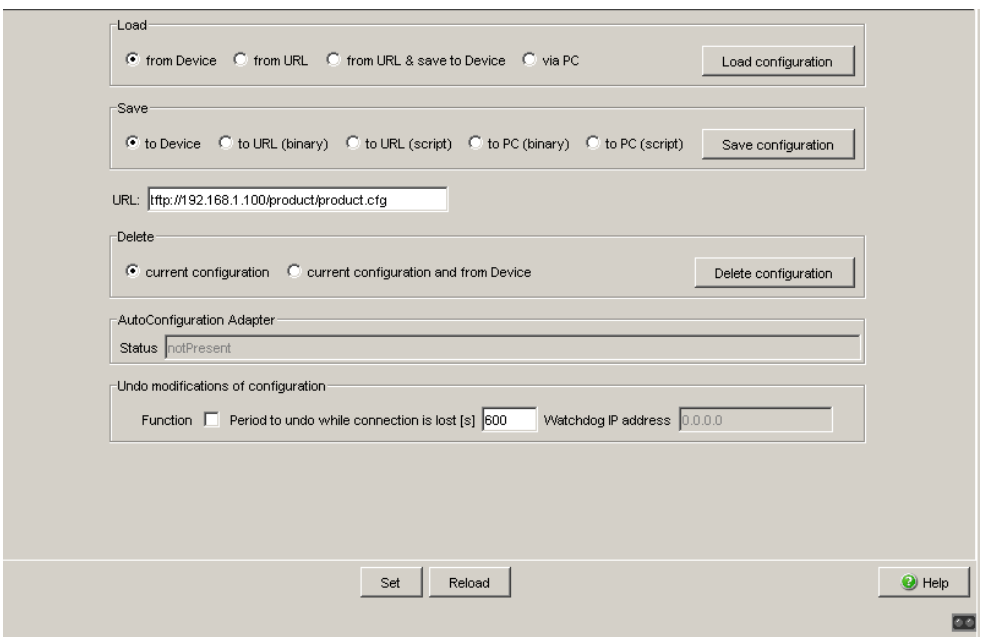


Figure 13: Load/Save dialog

1.6.1 Loading the configuration

In the "Load" frame, you have the option to

- load a configuration saved on the device,
- load a configuration stored under the specified URL,
- load a configuration stored on the specified URL and save it on the device,
- load a configuration saved on a PC in binary format.

If you change the current configuration (for example, by switching a port off), the load/save symbol in the menu area changes from a disk symbol into a yellow triangle. After saving the configuration, the load/save symbol changes back into the disk symbol.

1.6.2 Saving the configuration

In the "Save" frame, you have the option to

- save the current configuration on the device,
- save the current configuration in binary form in a file under the specified URL,
- save the current configuration in binary form on the PC,

Note: The loading process started by DHCP/BOOTP (see on page 21 „Network“) shows the selection of "from URL & save local" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

If you change the current configuration (for example, by switching a port off), the load/save symbol in the menu area changes from a disk symbol into a yellow triangle. After saving the configuration, the load/save symbol changes back into the disk symbol.

1.6.3 URL

The URL identifies the path to the tftp server on which the configuration file is to be stored. The URL is in the format: tftp://IP address of the tftp server/path name/file name (e.g. `tftp://192.168.1.100/product/config.dat`).
The configuration file includes all configuration data, including the password. Therefore pay attention to the access rights on the tftp server.

1.6.4 Deleting a configuration

In the "Delete" frame, you have the option to

- Reset the current configuration to the state on delivery. The configuration saved on the device is retained.
- Reset the to the state on delivery. After the next restart, the IP address is also in the state on delivery.

1.6.5 Using the AutoConfiguration Adapter (ACA)

The ACAs are devices for saving the configuration data of a device. In the case of a device failure, an ACA enables the configuration data to be transferred easily by means of a substitute device of the same type.

Note: If you replace a device with DIP switches, please ensure that the DIP switch settings are identical.

- **Storing the current configuration data in the ACA:**
  You have the option of transferring the current device configuration, including the SNMP password on the ACA and the flash memory in the "Save" frame using the "to Switch / Save configuration" option.

- **Transferring the configuration data from the ACA:**
  When you restart the device adopts the configuration data of the ACA and saves it permanently in the flash memory. If the connected ACA does not contain any valid data, for example, if it is completely new, the device loads the data from the flash memory.

  Note: Before loading the configuration data from the ACA, the device compares the password stored in the device with the password in the ACA configuration data.

  The device loads the configuration data if
  - The admin password matches or
  - There is no password stored locally or
  - The local password is the initial state of delivery password or
  - No configuration is saved locally.

Status	Meaning
notPresent	No ACA present.
ok	The configuration data from the ACA and the device are consistent.
removed	The ACA has been removed after booting.
notInSync	The configuration data from the ACA and the device are not consistent.
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in the ACA originates from a different device type and cannot be read or converted.
checksumErr	The configuration data is damaged.

Table 3: ACA status

1.6.6 Canceling a configuration change

Operation

If the function is activated and the connection to the device is interrupted for longer than the time specified in the field "Period to undo while connection is lost [s]", the device then loads the last configuration saved.

☐ Activate the function before you configure the device so that after an incorrect configuration has interrupted your connection to the device, you will be connected to the device again.

☐ Enter the "Period to undo while the connection is lost [s]" in seconds.
Possible values: 10-600 seconds.
Default setting: 600 seconds.

Note: Deactivate the function after you have successfully saved the configuration. You thus prevent the device from reloading the configuration after you close the web interface.

Watchdog IP address

"Watchdog IP address" shows you the IP address of the PC from which you have activated the (watchdog) function. The device monitors the link to the PC with this IP address, checking for interruptions.

1.7 Restart

With this dialog you can:

- Cold start the device. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- Warm start the device. In this case the device checks the software in the volatile memory and restarts.
- Reset the entries with the status "learned" in the filter table (MAC address table),
- Reset the ARP table (the device maintains an ARP table internally. If, for example, you assign a new IP address to a computer and subsequently have problems with the connection, you then reset the ARP table).
- Reset the port counters,
- Delete the log file.

Note: During the restart, the device temporarily does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems such as HiVision.

Figure 14: Restart dialog

2 Security

The security menu contains the dialogs, displays and tables for configuring the security settings:

- Password
- SNMPv1/v2 access
- Telnet/Web access
- Port security

2.1 Password / SNMP Access

This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface/CLI/SNMP. Please note that passwords are case-sensitive. For security reasons, the read password and the read/write password should not be identical.

The Web-based interface and the user interface communicate via SNMP version 3.

☐ Select "Modify read-only password (user) " to enter the read password.
☐ Enter the new read password in the "New password" line and repeat your entry in the "Please retype" line.
☐ Select "Modify read-write password (admin)" to enter the read/write password.
☐ Enter the read/write password and repeat your entry.

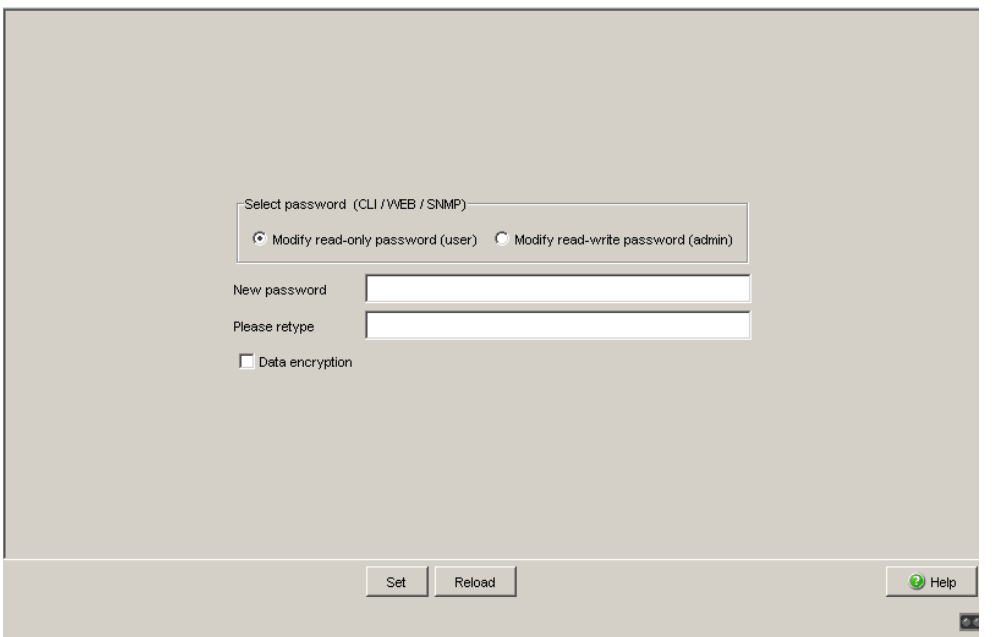


Figure 15: Password dialog

Important: If you do not know a password with “read/write” access, you will not have write access to the device!

Note: For security reasons, the passwords are not displayed. Make a note of every change! You cannot access the device without a valid password!

Note: For security reasons, SNMP version 3 encrypts the password. With the “SNMPv1” or “SNMPv2” setting in the Security:SNMPv1/v2 access dialog, the password is passed on unencrypted and can therefore also be read!

Note: In SNMP version 3, use between 5 and 32 characters for the password, because many applications do not accept shorter passwords.

Access via a Web browser or TELNET client can be blocked in a separate dialog (see on page 43 „Telnet/Web Access“).

Access at IP address level is restricted in a separate dialog (see on page 40 „SNMPv1/v2 Access Settings“).

2.2 SNMPv1/v2 Access Settings

With this dialog you can select access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated.
You can thus manage the device with HiVision and communicate with earlier versions of SNMP.
You can thus communicate with earlier versions of SNMP.

Note: For displaying the entries of the dialog you need read-write access.

- In the "Index" column, you enter the current number to which the access restriction applies.
- Enter the password with which this computer may access the device in the "Password" column. Please note that passwords are case-sensitive. This password is independent of the SNMPv3 password.
- In the "IP Address" column, you enter the IP address which may access the device. No entry in this field, or the entry "0.0.0.0", enables access to the device from computers with any IP address. In this case, the only access protection is the password.
- In the "IP Mask" column, much the same as with network masks, you can select a group of IP addresses.
  Example:
  255.255.255.255: a single IP address
  255.255.255.240 with IP address = 172.168.23.20:
  the IP addresses 172.168.23.16 to 172.168.23.31.

Binary notation of the mask 255.255.255.240:
1111 1111 1111 1111 1111 1111 1111 0000
mask bits
Binary notation of the IP address 172.168.23.20:
1010 1100 1010 1000 0001 0111 0001 0100

The binary representation of the mask with the IP address yields an address range of:
1010 1100 1010 1000 0001 0111 0001 0000 bis
1010 1100 1010 1000 0001 0111 0001 1111
i.e.: 172.168.23.16 to 172.168.23.31

- In the "Access Mode" column, you specify whether this computer can access the device with the read password or with the read/write password.
- You can activate/deactivate this table entry in the "Active" column.

Important: If no line is marked, then there are no access restrictions regarding the IP addresses!

- The "Create entry" button enables you to create a new row in the table.
- With "Delete entry" you delete the selected row in the table.

Note: The row with the password currently in use cannot be deleted or changed.

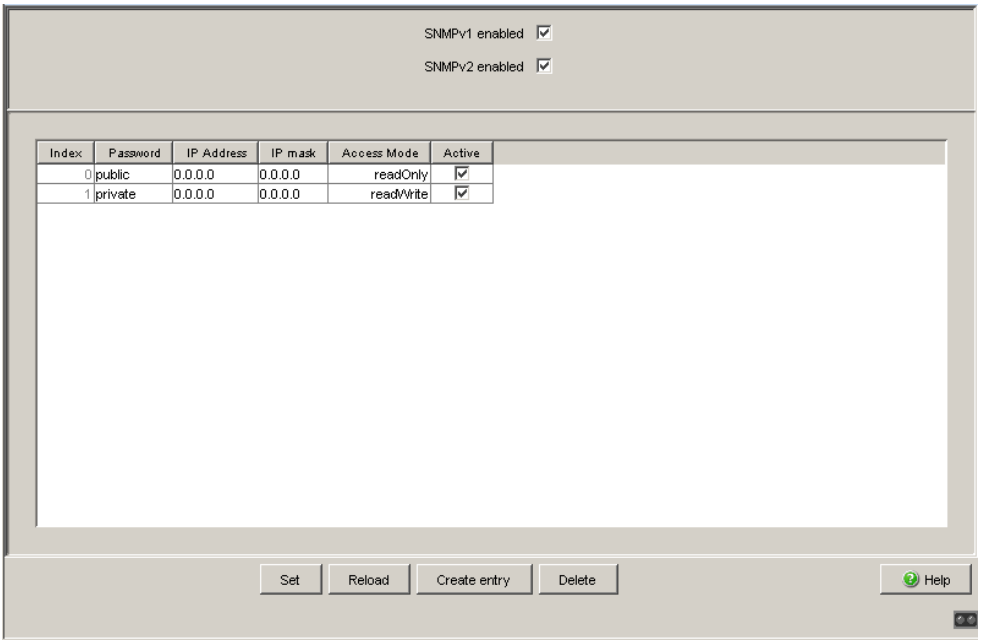


Figure 16: SNMPv1/v2 access dialog

2.3 Telnet/Web Access

This dialog allows you to switch off the Telnet server and the Web server on the device.

Figure 17: Telnet/Web access dialog

2.3.1 Description of Telnet access

The Telnet server of the device allows you to configure the device by using the Command Line Interface (in-band). You can deactivate the Telnet server to prevent Telnet access to the device.
On delivery, the server is activated.
After the Telnet server has been deactivated, you will no longer be able to access the device via a new Telnet connection. If a Telnet connection already exists, it is kept.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allow you to reactivate the Telnet server.

2.3.2 Description of Web access

The Web server of the device allows you to configure the device by using the Web-based interface. You can deactivate the Web server to prevent Web access to the device.
On delivery, the server is activated.

After the Web server has been switched off, it is no longer possible to login via a Web browser. The login in the open browser window remains active.

Note: The Command Line Interface and this dialog allow you to reactivate the Telnet server.

2.4 Port Security

The device protects every port from unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.

MAC-Based Port Security	Check source MAC address of a received data packet.
IP-Based Port Security	Check source IP address of a received data packet.

Table 4: Configuration for all ports

Name	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port Status	`enabled`: Port is switched on and transmitting. `disabled`: Port is switched off and not transmitting. The port is switched on if an authorized address accesses the port or `trapOnly` or `none` is selected under “Action” and an unauthorized address attempts to access the port. The port is switched off if `portDisable` is selected under “Action” and an unauthorized address attempts to access the port.
Allowed MAC Addresses	MAC addresses of the devices with which you allow data exchange at this port. The Web-based interface allows you to enter up to 10 MAC addresses, separated by a space character. After each MAC address you can enter a slash followed by a number identifying an address area. This number, between 2 and 47, indicates the number of relevant bits. Example: 00:80:63:01:02:00/40 stands for 00:80:63:01:02:00 to 00:80:63:01:02:FF or 00:80:63:00:00:00/24 stands for 00:80:63:00:00:00 to 00:80:63:FF:FF:FF If there is no entry, all devices can communicate via this port.

Table 5: Security per port

Name	Meaning
Current MAC Address	Shows the MAC address of the device from which the port last received data. The Web-based interface allows you to copy an entry from the “Current MAC Address” column into the “Allowed MAC Addresses” column using the left mouse button.
Allowed IP Addresses	IP addresses of the devices with which you allow data exchange at this port. The Web-based interface allows you to enter up to 10 IP addresses separated by a space character, or groups of IP addresses in mask form. If there is no entry, all devices can communicate via this port.
Action	Action performed by the device after an unauthorized access: – `none`: no action – `trapOnly`: send alarm – `portDisab`: disable the port with the corresponding entry in the port configuration table (see on page 25 „Port configuration“) and send an alarm

Table 5: Security per port

Note: This entry in the port configuration table is part of the configuration (see on page 29 „Load/Save“) and is saved together with the configuration.

Note: Prerequisites for the device to be able to send an alarm (trap) (see on page 143 „Alarms (Traps)“):
– You have entered at least one recipient
– You have set the flag in the “Active” column for at least one recipient
– In the “Selection” frame, you have selected “Port Security”

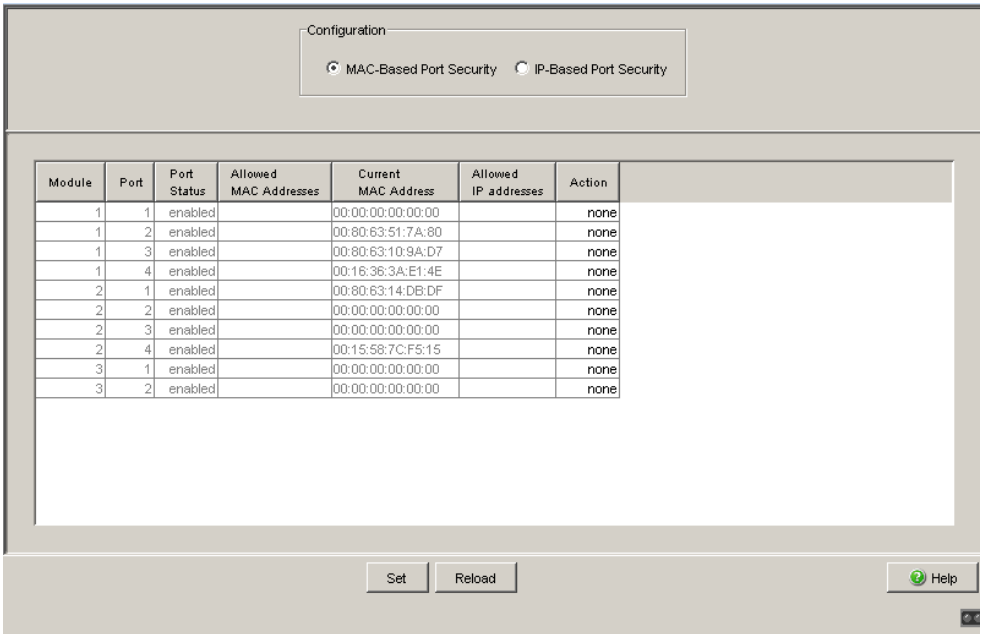


Figure 18: Port Security dialog

Note: Since the device is a layer 2 device, it translates the IP addresses entered into MAC addresses. For this, exactly one IP address must be assigned to a MAC address.
Please keep in mind that when using a router, for example, several IP addresses can be assigned to one MAC address, namely that of the router. This means that all packets of the router will pass the port unchecked if the permitted IP address is that of the router.
If a connected device sends packets with other MAC addresses and a permitted IP address, the device will disable the port.

3 Time

With this dialog you can enter time-related settings independently of the time synchronization protocol selected.

- The “IEEE/SNTP time” displays the time with reference to Universal Time Coordinated (UTC).
  The time displayed is the same worldwide. Local time differences are not taken into account.

- The “System time” uses the “IEEE 1588 / SNTP time”, allowing for the local time difference from “IEEE 1588 / SNTP time”.
  “System time” = “IEEE 1588 / SNTP time” + “Local offset”.

- “Time source” displays the source of the following time data. The device automatically selects the source with the greatest accuracy.

☐ With “Set time from PC”, the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
“IEEE 1588 / SNTP time” = “System time” - “Local offset”

- The “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTP time”.

☐ With “Set offset from PC”, the agent determines the time zone on your PC and uses it to calculate the local time difference.

Note: When setting the time in zones with summer and winter times, make an adjustment for the local offset. The device can also get the SNTP server IP address and the local offset from a DHCP server.

Interaction of PTP and SNTP
According to PTP (IEEE 1588) and SNTP, both protocols can exist in parallel in the same network. However, since both protocols affect the system time of the device, situations may occur in which the two protocols compete with each other.

The PTP reference clock gets its time either via SNTP or from its own clock. All other clocks favor using the PTP time as the source.

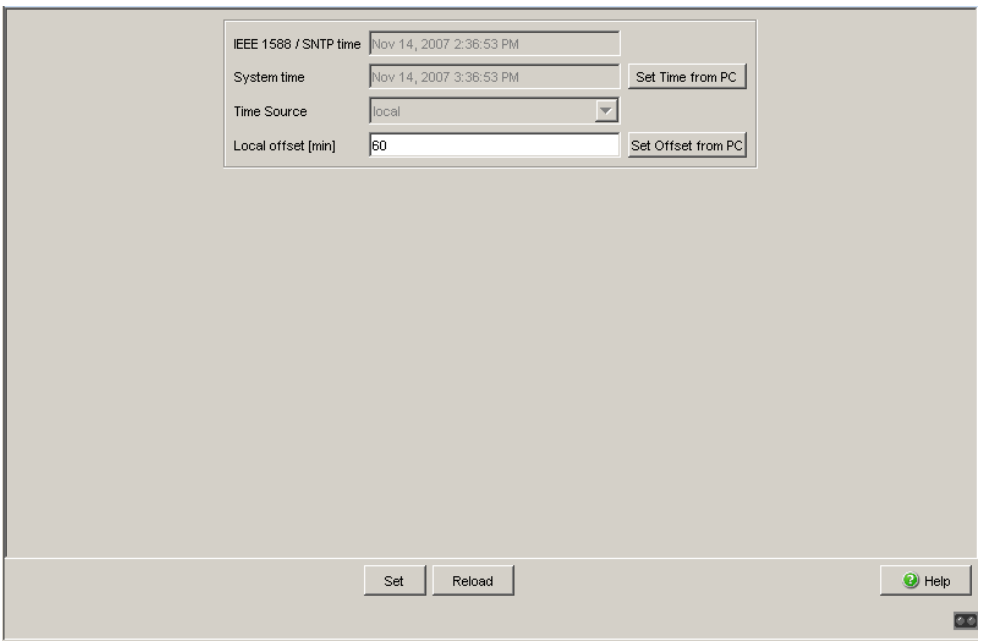


Figure 19: Time dialog

3.1 SNTP configuration

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP Server and SNTP Client functions.
The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account. The SNTP client obtains the UTC from the SNTP server.

Note: For the most accurate system time distribution possible, avoid having network components (routers,switches, hubs) which do not support SNTP in the signal path between the SNTP server and the SNTP client.

Parameter	Meaning
Function	Switch the SNTP function on and off In this frame you switch the SNTP function on/off. When it is switched off, the SNTP server does not send any SNTP packets or respond to any SNTP requests. The SNTP client does not send any SNTP requests or evaluate any SNTP Broadcast/Multicast packets.

Table 6: Configuration SNTP Client and Server

Parameter	Meaning
SNTP Status	The “Status message” displays conditions such as “Server cannot be reached”.

Table 7: SNTP Status

Parameter	Meaning
Anycast destination address	Enter the IP address to which the SNTP server on the device sends the SNTP packets.
VLAN ID	Enter the VLAN to which the device may periodically send SNTP packets.
Anycast send interval	Enter the time interval at which the device sends SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 120 seconds).
Disable Server at local time source	Enables/disables the SNTP server function if the status of the time source is “local” (see Time dialog).

Table 8: Configuration SNTP Server

IP destination address	Send SNTP packets periodically to
0.0.0.0	Nobody
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

Table 9: Periodic sending of SNTP packets

Parameter	Meaning
External server address	Enter the IP address of the SNTP server from which the device periodically requests the system time.
Redundant server address	Enter the IP address of the SNTP server from which the device periodically requests the system time, if it does not receive a response to a request from the “External server address” within 0.5 seconds.
Server request interval	Enter the time interval at which the device requests SNTP packets (valid entries: 1 second to 3600 seconds, on delivery: 30 seconds).
Accept SNTP Broadcasts	Specify whether the device accepts the system time from SNTP Broadcast/Multicast packets that it receives.
Threshold for obtaining the UTC	Reduces the frequency with which the time changes. Enter the threshold in milliseconds. The device changes the time as soon as the deviation from the server time is above this threshold.
Disable Client after successful synchronization	Enable/disable further time synchronizations once the device has synchronized its time with the server.

Table 10: Configuration SNTP Client

Note: If you are receiving the system time from an external/redundant server address, you do not accept any SNTP Broadcasts (see “Accept SNTP Broadcasts”). Otherwise you can never distinguish whether the device is displaying the time from the server entered, or that of an SNTP Broadcast packet.

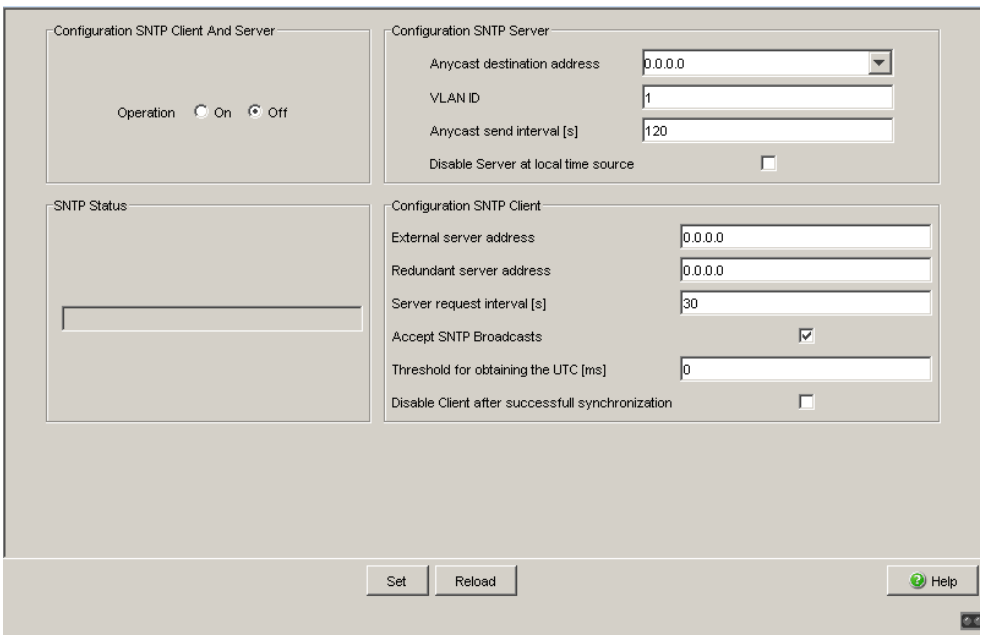


Figure 20: SNTP dialog

3.2 PTP (IEEE 1588)

Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that assumes one clock is the most accurate and thus enables precise synchronization of all clocks in an LAN.

For devices without a real-time (RT) module (timestamp unit):

- enable/disable the PTP function in the `PTP` dialog.
- select the PTP mode in the `PTP` dialog.
  - Select `v1-simple-mode` if the reference clock uses PTP version 1.
  - Select `v2-simple-mode` if the reference clock uses PTP version 2.

The following sections relate to devices that support real-time (RT) modules (timestamp unit).

3.2.1 PTP Global (MS20/MS30, PowerMICE)

The table below helps you to select the PTP version and the PTP mode.

Version	Mode	Reference clock used	Device with timestamp	PTP messages
Version 1	v1-simple-mode	Version 1	No	—
	v1-boundary-clock	Version 1	Yes	Process
Version 2	v2-simple-mode	Version 2	No	—
	v2-boundary-clock-onestep	Version 2	Yes	Process
	v2-boundary-clock-twostep	Version 2	Yes	Process
	v2-transparent-clock	Version 2	Yes	Forward

Table 11: Selecting the PTP version and the PTP mode

The PTP modes
- v1-boundary-clock,
- v2-boundary-clock-onestep,
- v2-boundary-clock-twostep and
- v2-transparent-clock

enable you to optimize the accuracy of the time.

You use these dialogs here
- Version 1
- Version 2 (Boundary Clock, BC)
- Version 2 Transparent Clock, (TC)

The PTP modes
- v1-simple-mode and
- v2-simple-mode

allow you to use the plug-and-play start-up.

Parameter	Meaning	Value range	Default setting
Function on/off	Enable/disable the PTP function	On, Off	Off

Table 12: Function IEEE 1588/PTP

Parameter	Meaning	Value range	Default setting
PTP version/ mode	Version and mode of the local clock.		v1-boundary-clock
	Boundary Clock function based on IEEE1588-2002 (PTPv1).	v1-boundary-clock	
	Support for PTPv1 without special hardware. The device synchronizes itself with received PTPv1 messages. This mode does not provide any other functions, such as PTP management or runtime measuring. Select this mode if the device does not have a timestamp unit (RT module).	v1-simple-mode	
	Boundary Clock function based on IEEE1588-2008 (PTPv2). The one-step mode determines the precise PTP time with one message. This mode is available for MM23 and MM33 modules.	v2-boundary-clock-onestep	
	Boundary Clock function based on IEEE1588-2008 (PTPv2). The two-step mode determines the precise PTP time with two messages.	v2-boundary-clock-twostep	
	Transparent Clock (one-step) function based on IEEE1588-2008 (PTPv2). This mode is available for MM23 and MM33 modules.	v2-transparent-clock	
	Support for PTPv2 without special hardware. The device synchronizes itself with received PTPv2 messages. This mode does not provide any other functions, such as PTP management or runtime measuring. Select this mode if the device does not have a timestamp unit (RT module).	v2-simple-mode	

Table 13: Configuration IEEE 1588/PTP

Parameter	Meaning	Value range	Default setting
Bottom synchronization threshold [ns]	Bottom PTP synchronization threshold value, specified in nanoseconds. If the result of (reference time - local time) is lower than the value of the bottom PTP synchronization threshold, then the local clock is deemed as synchronous with the reference clock.	0-999999999	30
Top synchronization threshold [ns]	Top PTP synchronization threshold value, specified in nanoseconds. If the result of (reference time - local time) is greater than the value of the top PTP synchronization threshold, then the local clock is deemed as not being synchronous with the reference clock.	31-1000000000	5000

Table 13: Configuration IEEE 1588/PTP

Parameter	Meaning	Value range	Default setting
Is synchronized	Local clock synchronized with reference clock; compare `Bottom synchronization threshold` and `Top synchronization threshold`.	true false	
Max Offset absolute [ns]	Total deviation of the local clock from the reference clock in nanoseconds since the local clock was last reset. The local clock is reset with “Reinitialize” in this dialog or by resetting the device.		

Table 14: IEEE 1588/PTPStatus

3.2.2 PTP Version 1 (MS20/MS30, Power MICE)

You select the PTP version you want to use in the `Time:PTP:Global` dialog.

PTP Version 1, Global Settings

Parameter	Meaning	Value range	Default setting
Sync Interval	Period for sending synchronization messages. Entered in seconds.	- sec-1 - sec-2 - sec-8 - sec-16 - sec-64	sec-2
Subdomain name	Name of the PTP subdomain to which the local clock belongs.	5 ASCII characters	_DFLT
Preferred Master	Defines the local clock as the preferred master. If PTP does not find another preferred master, then the local clock is used as the grandmaster clock. If PTP finds other preferred masters, then PTP determines which of the preferred masters is used as the grandmaster clock.	true false	false

Table 15: Function IEEE 1588/PTPv1

Parameter	Meaning	Value range	Default setting
Offset to Master [ns]	Deviation of the local clock from the reference clock in nanoseconds.		
Runtime to Master [ns]	Single signal runtime between the local device and reference clock in nanoseconds.		
Grandmaster UUID	MAC address of the grandmaster clock (Unique Universal Identifier).		
Parent UUID	MAC address of the master clock with which the local time is directly synchronized.		
Clock Stratum	Qualification of the local clock.		
Clock identifier	Clock properties (e.g accuracy, epoch, etc.).		

Table 16: Status IEEE 1588/PTPv1

PTP Version 1, Port Settings

Parameter	Meaning	Value range	Default setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. The table remains empty if the device does not support the PTP mode selected		
PTP on	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages.	off	
PTP Burst on	2 to 8 synchronization runs take place during the synchronization interval. This enables faster synchronization with a correspondingly higher network load.	on	off
	One synchronization run is performed in a synchronization interval.	off	
PTP Status	Port is in the initialization phase.	initializing	
	Port fault. Error in the PTP protocol.	faulty	
	PTP function is switched off at this port.	disabled	
	Port has not received any information and is waiting for synchronization messages.	listening	
	Port is in PTP pre-master mode.	pre-master	
	Port is in PTP master mode.	master	
	Port is in PTP passive mode.	passive	
	Port is in PTP uncalibrated mode.	uncalibrated	
	Port is in PTP slave mode.	slave	

Table 17: Port dialog version 1

3.2.3 PTP Version 2 (BC) (MS20/MS30, PowerMICE)

PTP version 2 provides considerably more setting options. These enable
- faster reconfiguration of the PTP network than in PTP version 1
- greater precision in some environments.

You select the PTP version you want to use in the `Time:PTP:Global` dialog.

PTP Version 2 (TC), Global Settings

Parameter	Meaning	Value range	Default setting
Priority 1	The clock with the lowest priority 1 becomes the reference clock (grandmaster).	0-255	128
Priority 2	If all the relevant values for selecting the reference clock are the same for multiple devices, the clock with the lowest priority 2 is selected as the reference clock (grandmaster).	0-255	128
Domain number	Assignment of the clock to a PTPv2 domain. Only clocks with the same domain are synchronized.	0-255	0

Table 18: Function IEEE 1588/PTPv2 BC

Parameter	Meaning	Value range	Default setting
Two Step	Displays the clock mode of the device		No
	v2-boundary-clock-onestep	No	
	v2-boundary-clock-twostep	Yes	
Number of BCs to grandmaster	Number of boundary clocks between PTP reference clock and this device		
Offset to Master [ns]	Deviation of the local clock from the reference clock in nanoseconds.		
Runtime to Master [ns]	Single signal runtime between the local device and the reference clock in nanoseconds. The display depends on the port setting “Runtime measuring mechanism”.		

Table 19: Status IEEE 1588/PTPv2 BC

Parameter	Meaning	Value range	Default setting
Clock identifier	Own UUID (unique identification number)		
Parent port identifier	UUID of the direct master		
Grandmaster identifier	UUID of the reference clock		

Table 20: Identifiers

Parameter	Meaning	Value range	Default setting
Priority 1	Display priority 1 of the current reference clock.		
Priority 2	Display priority 2 of the current reference clock.		
Class	Class of the reference clock		
Precision	Estimated accuracy with regard to UTC		
Variance	Variance as described in the IEEE1588-2008 standard		

Table 21: Grandmaster (reference clock)

Parameter	Meaning	Value range	Default setting
Time source	Source selected for own clock.	atomicClock gps terrestrialRadio ptp ntp handset other internalOscillator	internalOscilla-tor
UTC Offset [s]	Current difference between the PTP time scale (see below) and the UTC.	-2147483648 to 2147483647	34
UTC Offset valid	Specifies whether value of UTC off-set is valid or not.	Yes, No	No
Time Traceable	The device gets the time from a pri-mary UTC reference, e.g. from an NTP server.	Yes No	
Frequency Traceable	The device gets the frequency from a primary UTC reference, e.g. NTP server, GPS.	Yes No	
PTP Time Scale	The device uses the PTP time scale. According to IEEE 1588, the PTP time scale is the TAI atomic time started on 01.01.1970. In contrast to UTC, TAI does not use leap sec-onds. On 01.01.2009, the difference between UTC and TAI was 34 sec-onds.	Yes No	

Table 22: Properties of the local time

PTP Version 2 (TC), Port Settings

Parameter	Meaning	Value range	Default setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. The table remains empty if the device does not support the PTP mode selected		
PTP on	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages.	off	
PTP Status	Port is in the initialization phase.	initializing	
	Port fault. Error in the PTP protocol.	faulty	
	PTP function is switched off at this port.	disabled	
	Port has not received any information and is waiting for synchronization messages.	listening	
	Port is in PTP pre-master mode.	pre-master	
	Port is in PTP master mode.	master	
	Port is in PTP passive mode.	passive	
	Port is in PTP uncalibrated mode.	uncalibrated	
	Port is in PTP slave mode.	slave	
E2E Runtime Measuring Interval	Displays in seconds the interval for E2E runtime measurements at this port. This is a value for the device, assigned to ports with the PTP status Slave by the connected master. If the port itself is the master, then the device assigns the port the value 8 (state on delivery).		8
P2P Runtime	Measured peer-to-peer runtime. Prerequisite: you have selected the P2P runtime measuring mechanism.		
Announce Interval	Interval of the messages for PTP topology discovery (selection of the reference clock). Select the same value for all devices within a PTP domain.	1, 2, 4, 8, 16	2

Table 23: Port Dialog Version 2(BC)

Parameter	Meaning	Value range	Default setting
Announce Timeout	Announce interval timeout for PTP topology discovery in number of announce intervals. The standard settings of announce interval = 2 (2 per second) and announce timeout = 3 lead to a timeout of 3 x 2 seconds = 6 seconds. Select the same value for all devices within a PTP domain.	2-10	3
Sync Interval	Interval in seconds for the synchronization messages	0,5, 1, 2	1
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	The device itself does not generate any messages in the runtime measurement. A connected PTP slave measures the runtime of the entire transmission path to the master.	E2E (end-to-end):	
	The device itself measures the runtime to all the connected PTP devices. If a reconfiguration is performed, this removes the need to determine the runtime again. The MICE media modules MM23 and MM33 support the P2P mechanism.	P2P (peer-to-peer)	
	No runtime determination.	Disabled	
P2P Runtime Measuring Interval	Interval for peer-to-peer runtime measurements at this port. Prerequisite: You have selected the P2P runtime measuring mechanism on the device itself and on the connected PTP device.		
Network Protocol	Transport protocol for all PTP messages.	- 802.3 Ethernet - UDP/- IPv4	

Table 23: Port Dialog Version 2(BC)

Parameter	Meaning	Value range	Default setting
V1 Hardware Compatibility	Some devices from other manufacturers require PTP messages of specific length. If the UDP/IPv4 network protocol is selected and the function is active, the device extends the PTP messages.	auto, on, off	auto
Asymmetry	Correction of the runtime asymmetry in [ns]. A runtime measurement value of x ns corrupted by asymmetrical transmission values corresponds to an asymmetry of x*2 ns		

Table 23: Port Dialog Version 2(BC)

3.2.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE)

In strongly cascaded networks in particular, the transparent clock (TC) introduced in PTP Version 2 provides a noticeable increase in precision.
The combination with the P2P runtime mechanism (simultaneous runtime measurement at all ports) enables “seamless” reconfiguration.

The following settings enable you to also use the TC for Unicast PTP messages:
– Selecting the E2E mechanism
– Syntonize disabled
– PTP Management disabled.

You select the PTP version you want to use in the `Time:PTP:Global` dialog.

PTP Version 2 (TC), Global Settings

Parameter	Meaning	Value range	Default setting
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	The device itself does not generate any messages in the runtime measurement. A connected PTP slave measures the runtime of the entire transmission path to the master.	E2E (end-to-end):	
	The device itself measures the runtime to all the connected PTP devices. If a reconfiguration is performed, this removes the need to determine the runtime again.	P2P (peer-to-peer)	
Primary Domain	Assignment of the clock to a PTPv2 domain.	0-225	
Multi Domain Mode	TC corrects messages from all domains.	Yes	Yes
	TC only corrects messages from the primary domain.	No	
Network Protocol	Network protocol for P2P and management messages.	udplpv4 ieee8023	udplpv4
Syntonize	Synchronize frequency.	Yes No	No
PTP Management	Activate/deactivate the PTP management. To reduce the load on the device, deactivate PTP Management and Syntonize - at high synchronization rates and - in Unicast mode.	Yes No	Yes

Table 24: Function IEEE 1588 / PTPv2 TC

Parameter	Meaning	Value range	Default setting
Clock identifier	UUID of the TC (transparent clock)		
Current master	If Syntonize is enabled, displays the UUID of the master with which the device synchronizes its frequency.		

Table 25: Status IEEE 1588 / PTPv2 TC

PTP Version 2 (TC) Port Settings

Parameter	Meaning	Value range	Default setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. The table remains empty if the device does not support the PTP mode selected		
PTP on	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages. The device does not process any PTP messages it receives at this port.	off	
P2P Runtime Measuring Interval	Interval for peer-to-peer runtime measurements at this port. Prerequisite: You have selected the P2P runtime measuring mechanism on the device itself and on the connected PTP device.		
P2P Runtime	Measured peer-to-peer runtime. Prerequisite: you have selected the P2P runtime measuring mechanism.		
Asymmetry	Correction of the runtime asymmetry in [ns]. A runtime measurement value of x ns corrupted by asymmetrical transmission values corresponds to an asymmetry of x*2 ns		

Table 26: Port Dialog Version 2(TC)

4 Switching

The switching menu contains the dialogs, displays and tables for configuring the switching settings:

- Switching Global
- Filters for MAC Addresses
- Rate Limiter
- Multicasts
- VLAN

4.1 Switching Global

Variable	Meaning	Possible values	State on delivery
MAC address	Display the MAC address of the device		
Aging Time (s)	Enter the Aging Time for all dynamic entries in seconds. In connection with the router redundancy (see MACH 3000), select a time greater than/equal to 30 seconds.	15-3825	30
Flow control	Activate/deactivate the flow control	on, off	off
Learning addresses	Activate/deactivate the address learning	on, off	on
Frame size	Set the maximum packet size (frame size). Select the larger value if you want the device to transmit packets with double tagging. You can thus operate the device in networks with MPLS switches/routers, for example.	1522, 1632	1522

Table 27: Switching:Global dialog

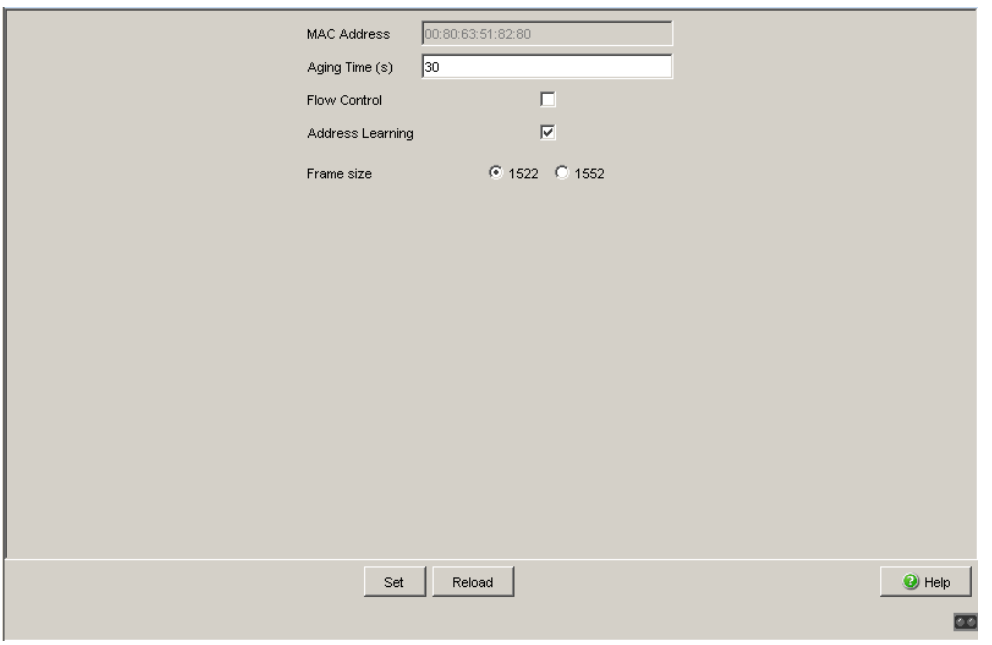


Figure 21: Switching Global

4.2 Filters for MAC addresses

The filter table for MAC addresses is used to display and edit filters. Each row represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the device (learned status) or manually. Data packets whose destination address is entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination address is not in the table are sent from the receiving port to all other ports. The following status settings are possible:

- `learned`: the filter was created automatically by the device.
- `invalid`: with this status you delete a manually created filter.
- `permanent`: the filter is stored permanently in the device or on the URL (see on page 29 „Load/Save“).
- `gmrp`: the filter was created by GMRP.
- `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart .
- `igmp`: the filter was created by IGMP.

In the “Create” dialog (see buttons below), you can create new filters.

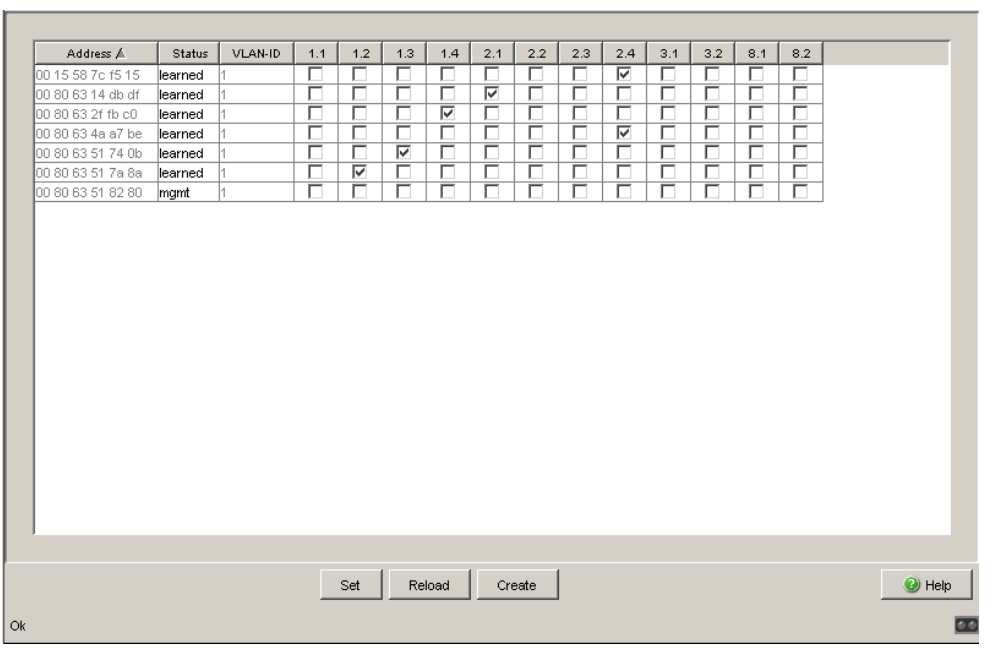


Figure 22: Filter Table dialog

Note: This filter table allows you to create up to 100 filters for Multicast addresses.

4.3 Rate Limiter

To ensure reliable data exchange during heavy traffic, the device can limit the traffic.

Entering a limit rate for each port specifies the amount of traffic the device is permitted to transmit and receive.

If the data load transmitted at this port exceeds the maximum load entered, the device will discard the excess data at this port.

A global setting enables/disables the rate limiter function at all ports.

4.3.1 Rate Limiter settings

- "Ingress Limiter (kbit/s)" allows you to enable or disable the input limiting function for all ports.
- "Egress Limiter (Pkt/s)" allows you to enable or disable the broadcast output limiter function at all ports.
- "Egress Limiter (kbit/s)" allows you to enable or disable the output limiter function for all packet types at all ports.

Setting options per port:

- "Ingress Packet Types" allows you to select the packet type for which the limit is to apply:
  - `All`, limits the total inbound data volume at this port.
  - `BC`, limits the broadcast packets received at this port.
  - `BC + MC`, limits broadcast packets and Multicast packets received at this port.
  - `BC + MC + uUC`, limits broadcast packets, Multicast packets, and unknown Unicast packets received at this port.
- Ingress Limiter Rate for the inbound packet type selected:
  - = 0, no ingress limit at this port.

- > 0, maximum inbound traffic rate in kbit/s that can be received at this port.

- Egress Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second that can be sent at this port.

- Egress Limiter Rate for the entire data stream:
  - = 0, no rate limit for outbound data stream at this port.
  - > 0, maximum outbound transmission rate in kbit/s sent at this port.

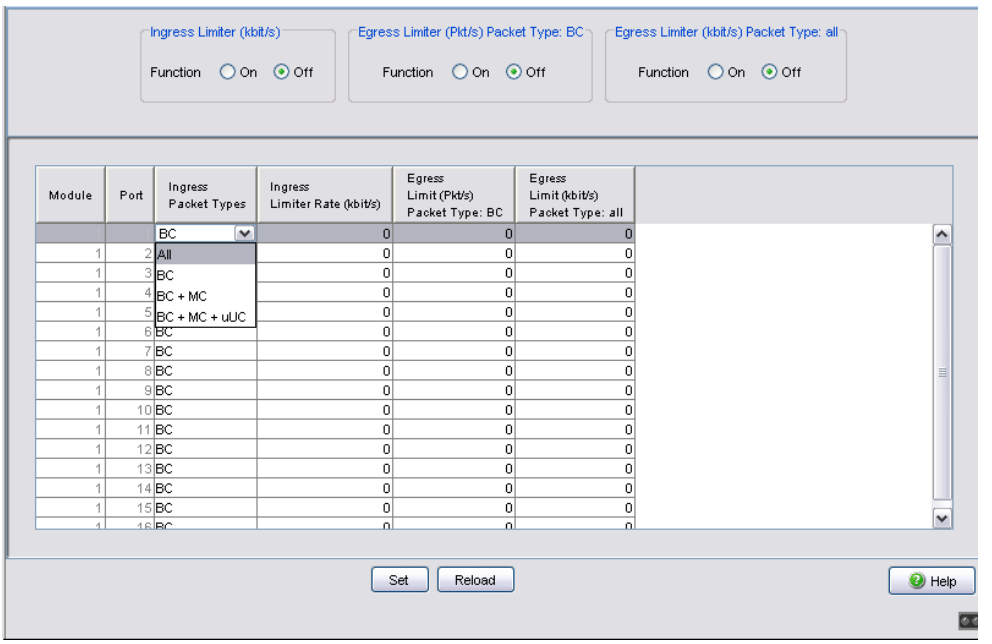


Figure 23: Rate Limiter dialog

4.4 Multicasts

With this dialog you can:
- activate/deactivate the IGMP protocol,
- configure the IGMP protocol globally and per port.

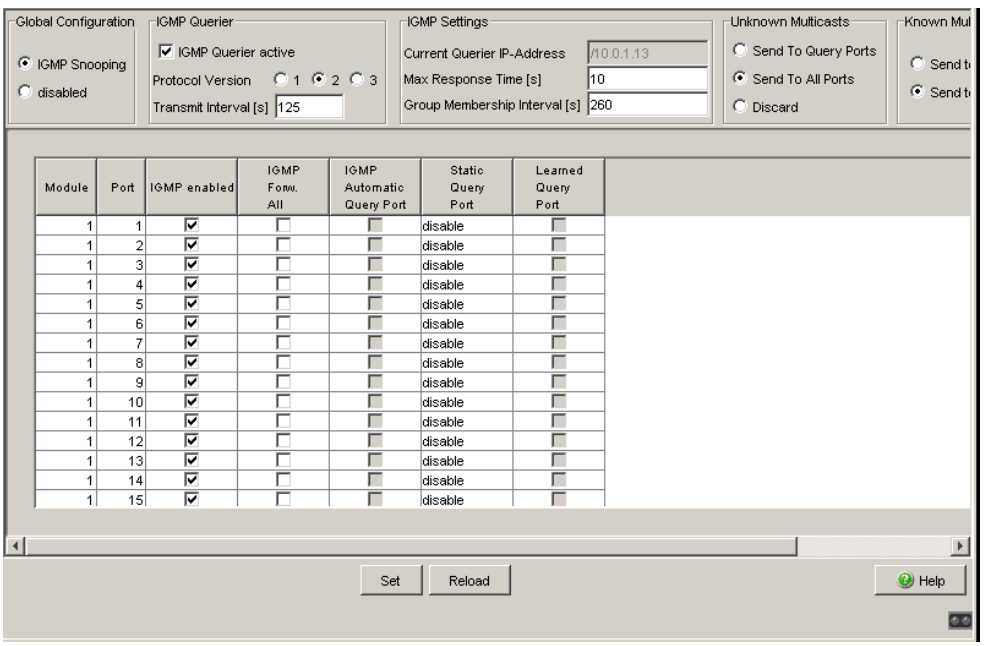


Figure 24: Multicasts dialog

4.4.1 Global Configuration

In this frame you can:
- activate/deactivate the IGMP protocol.

Parameter	Meaning	Default setting
IGMP Snooping	Activate IGMP Snooping globally for the entire device.	deselected
disabled	Deactivate IGMP Snooping globally for the entire device. If IGMP Snooping is switched off, then ▶ the device does not evaluate Query and Report packets received, and ▶ it sends (floods) received data packets with a Multicast address as the destination address to all ports.	selected

Table 28: Global setting

4.4.2 IGMP Querier and IGMP settings

With these frames you can enter global settings for the IGMP settings. Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.

Parameter	Meaning	Value range	Default setting
IGMP Querier			
IGMP Querier enabled	Switch query function on/off	on/off	off
Protocol Version	Select IGMP version 1, 2 or 3.	1, 2, 3	2
Send Interval	Enter the interval at which the switch sends query packets. All IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.	2-3599 s[a]	125 s
IGMP settings			
Current querier IP address	Display the IP address of the router/ switch that contains the query function.		
Max. Response Time	Enter the time within which the Multicast group members respond to a query. The Multicast group members select a random value within the response time for their response, to prevent all the Multicast group members responding to the query at the same time.	Protocol Version - 1,2: 1-25 s[a] - 3: 1-3598 s[a]	10 s
Group Membership Interval	Enter the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages.	3-3600 s[a]	260 s

Table 29: IGMP Querier and IGMP settings
a.) Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval, (see table 30)

The parameters
– Max. Response Time,
– Send Interval and
– Group Membership Interval
have a relationship to each other:

Max. Response Time < Send Interval < Group Membership Interval.

If you enter values that contradict this relationship, the device then replaces these values with a default value or with the last valid values.

Parameter	Protocol Version	Value range	Default setting
Max. Response Time	1, 2 3	1-25 seconds 1-3598 seconds	10 seconds
Send Interval	1, 2, 3	2-3599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3600 seconds	260 seconds

Table 30: Value range for
- Max. Response Time
- Send Interval
- Group Membership Interval

For “Send Interval” and “Max. Response Time”,
– select a large value if you want to reduce the load on your network and can accept the resulting longer switching times,
– select a small value if you require short switching times and can accept the resulting network load.

4.4.3 Unknown Multicasts

In this frame you define how the device sends packets with an unknown MAC/IP Multicast address that was not learned through IGMP Snooping. Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.

Parameter	Meaning	Value range	Default setting
Send to Query Ports	The device sends the packets with an unknown MAC/IP Multicast address to all query ports.	selected/deselected	deselected
Send to All Ports	The device sends the packets with an unknown MAC/IP Multicast address to all ports.	selected/deselected	selected
Discard	The device discards all packets with an unknown MAC/IP Multicast address.	selected/deselected	deselected

Table 31: Unknown Multicasts

Note: The way in which unlearned Multicast addresses are handled also applies to the reserved addresses from the “Local Network Control Block” (224.0.0.0 - 224.0.0.255). This can have an effect on higher-level routing protocols.

4.4.4 Known Multicasts

In this frame you define how the device sends packets with a known MAC/IP Multicast address that was learned through IGMP Snooping.
Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.

Parameter	Meaning	Value range	Default setting
Send to query and registered ports	The device sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports. This standard setting sends all Multicasts to all query ports and to registered ports. The advantage of this is that it works in most applications without any additional configuration. Application: “Flood and Prune” routing in PIM-DM.	selected/deselected	deselected
Send to registered ports	The device sends the packets with a known MAC/IP Multicast address to registered ports. The advantage of this setting, which deviates from the standard, is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings. Application: Routing protocol PIM-SM.	selected/deselected	selected

Table 32: Known Multicasts

4.4.5 Settings per port (table)

With this configuration table you can enter port-related IGMP or GMRP settings.

Parameter	Meaning	Value range	Default setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies.		
IGMP on	Switch IGMP on/off for each port. Switching IGMP off at a port prevents registration for this port. Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.	on/off	on
IGMP Forward All	Switch the IGMP Snooping function “Forward All” on/off With the “IGMP Forward All” setting, the device sends to this port all data packets with a Multicast address in the destination address field. Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected. **Note:** If a number of routers are connected to a subnetwork, you must use IGMP version 1 so that all the routers receive all the IGMP reports. **Note:** If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.	on/off	off
IGMP Automatic Query Port	Displays which ports the device has learned as query ports, if “automatic” is selected in “Static Query Port”. Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.	Yes/No	

Table 33: Settings per port

Parameter	Meaning	Value range	Default setting
Static Query Port	The device sends IGMP report messages to the ports at which it receives IGMP queries (default setting). This column allows you to also send IGMP report messages to: other selected ports (enable) or connected Hirschmann devices (automatic). Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.	enable, disable, automatic	disable
Learned Query Port	Shows at which ports the device has received IGMP queries, if “disable” is selected in “Static Query Port”. Prerequisite: In the `Switching:Multicasts:Global Settings` dialog, the `IGMP Snooping` mode is selected.	Yes/No	

Table 33: Settings per port

Note: If the device is connected to a HIPER-Ring, in the case of a ring interruption you can ensure quick reconfiguration of the network for data packets with registered Multicast destination addresses by:

- enabling IGMP on the ring ports and globally, and
- enabling "IGMP Forward All" per port on the ring ports.

4.5 VLAN

Under VLAN you will find all the dialogs and attributes for configuring and monitoring the VLAN function in accordance with the IEEE 802.1Q standard.

4.5.1 VLAN Global

With this dialog you can:

- display VLAN parameters
- activate/deactivate the VLAN 0 transparent mode
- configure and display the learning mode
- reset the VLAN settings of the device to the state on delivery.

Parameter	Meaning
Biggest VLAN ID	Displays the biggest possible VLAN ID (see on page 88 „VLAN Static“).
Max. Number of VLANs	Displays the maximum number of VLANs (see on page 88 „VLAN Static“).
VLANs configured	Displays the number of configured VLANs (see on page 88 „VLAN Static“).

Table 34: VLAN display

Note: The device provides the VLAN with the ID 1. The VLAN with ID 1 is always present.

Parameter	Meaning	Value range	Default setting
VLAN 0 Transparent Mode	When this is activated, the VLAN ID “0” remains in the packet, regardless of the setting for the port VLAN ID in the dialog (see on page 90 „VLAN Port“). Activate the “VLAN 0 Transparent Mode” to transmit packets with a priority TAG without VLAN membership, that is with VLAN ID “0”.	on/off	off

Table 35: VLAN settings

Note: If you are using the GOOSE protocol in accordance with IEC61850-8-1, you activate the “VLAN 0 transparent mode”. Thus the prioritizing information remains in the data packet in accordance with IEEE802.1D/p even when the device forwards the data packet.
This also applies to other protocols that use this prioritizing in accordance with IEEE802.1D/p but that do not require any VLANs in accordance with IEEE802.1Q.

Note: When using the “Transparent Mode” in this way, note the following:

- For RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS:
  In “Transparent mode”, the devices ignore the port VLAN ID set. Set the VLAN membership of the ports of VLAN 1 to `U` (Untagged) or `T` (Tagged), (see on page 88 „VLAN Static“).

Parameter	Meaning	Value range	Default setting
Mode	VLAN mode selection. **„Independent VLAN“** subdivides the forwarding database (see on page 71 „Filters for MAC addresses“) virtually into one independent forwarding database per VLAN. The device cannot assign data packets with a destination address in another VLAN, and so floods it to all ports of the VLAN. **Application area:** Setting up identical networks that use the same MAC addresses. **„Shared VLAN“** uses the same forwarding database for all VLANs (see on page 71 „Filters for MAC addresses“). The device cannot assign data packets with a destination address in another VLAN, and so only forwards them to the destination port if the receiving port is also a member of the VLAN group of the destination port. **Application area:** In the case of overlapping groups, the device can distribute directly across VLANs, as long as the ports involved belong to a VLAN that can be reached. Changes to the mode are only taken over after a warm start (see on page 35 „Restart“) is performed on the device, and the changes are then displayed in the line below under “Status”.	Independent VLAN, Shared VLAN	Independent VLAN
Status	Displays the current status. After a warm start (see on page 35 „Restart“) on the device, the device take the setting for the “Mode” into the status line.	Independent VLAN, Shared VLAN	

Table 36: Settings and displays in the “Learning” frame

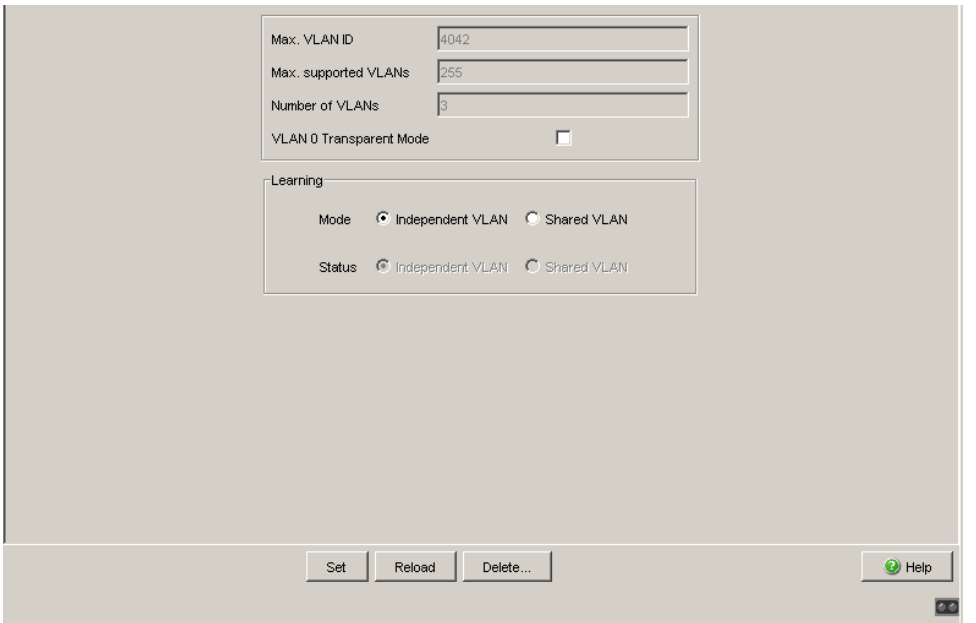


Figure 25: VLAN Global dialog

Figure 26: VLAN Global dialog

4.5.2 Current VLAN

With this dialog you can:

- display VLAN parameters

The Current VLAN table shows all
– manually configured VLANs
– VLANs configured via redundancy mechanisms
The Current VLAN table is only used for information purposes. You can make changes to the entries in the `VLAN:Static` dialog.

Parameter	Meaning	Value range
VLAN ID	Displays the ID of the VLAN.	
Status	Displays the VLAN status.	`other`: This entry solely appears for VLAN 1. The system provides VLAN 1. VLAN 1 is always present. `permanent`: A static entry made by you. This entry is kept when the device is restarted. dynamic: This VLAN was created dynamically via GVRP.
Time created	Operating time (see „System data“) at which the VLAN was created.	
Ports x.x	VLAN membership of the relevant port and handling of the VLAN tag.	– Currently not a member `T` Member of VLAN; send data packets with tag. `U` Member of the VLAN; send data packets without tag (untagged). `F` Membership forbidden, so no entry possible via GVRP either.

Table 37: Current VLAN

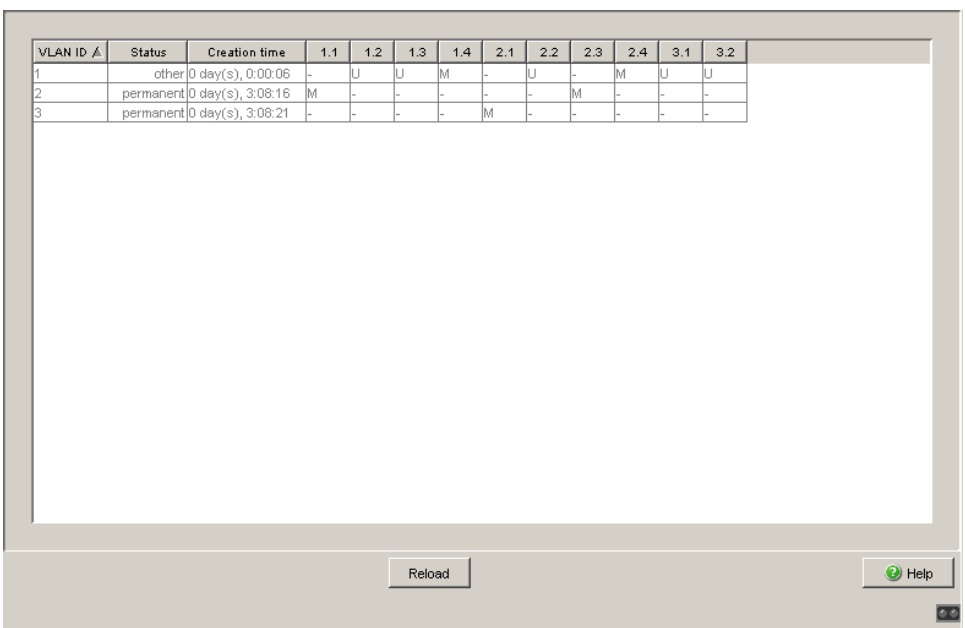


Figure 27: VLAN Current view

4.5.3 VLAN Static

With this dialog you can:

- Create VLANs
- Assign names to VLANs
- Assign ports to VLANs and configure them
- Delete VLANs

Parameter	Meaning	Value range	Default setting
VLAN ID	Displays the ID of up to 255 VLANs that are possible.	1-4042	
Name	Enter the name of your choice for this VLAN.	Maximum 32 characters	VLAN 1: default
Status	Displays the VLAN status.	**active** = entry is activated **notInService**= entry is deactivated	active
Ports x.x	Select the membership of the ports to the VLANs.	– currently not a member (GVRP allowed) T Member of VLAN; send data packets with tag. U Member of the VLAN; send data packets without tag (untagged). F Membership forbidden, so no entry possible via GVRP either.	VLAN 1: U new VLANs: –

Table 38: VLAN Static dialog

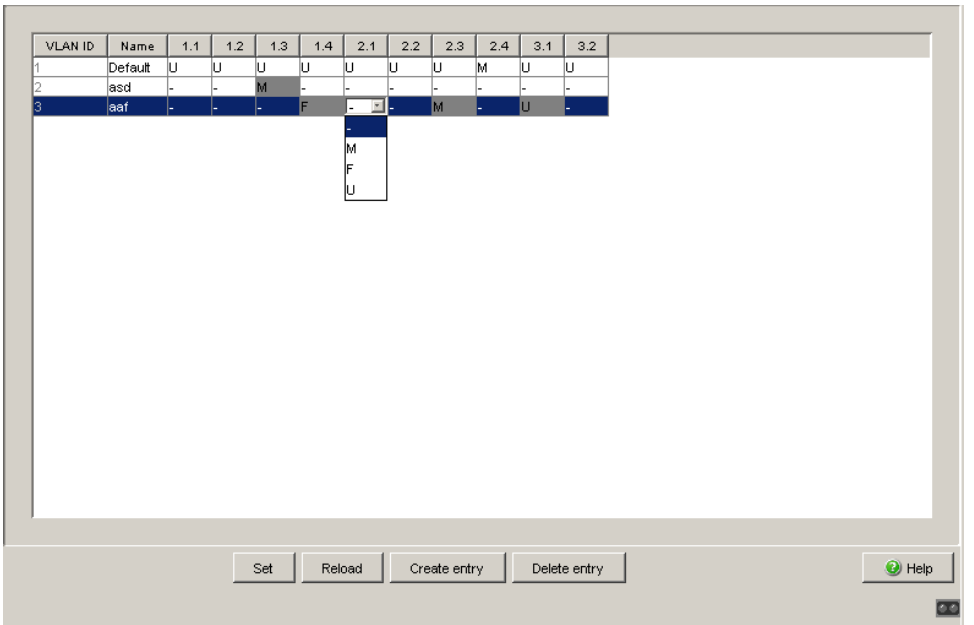


Figure 28: VLAN Static dialog

Note: When configuring the VLAN, ensure that the management station still has access to the device after the VLAN configuration is saved.
You achieve this by connecting the management station to a port with the VLAN ID 1. The device transmits the data of the management station in VLAN 1.

Note: The device automatically creates VLANs for MRP rings. Deleting these VLANs prevents the MRP-Ring function.

Note: Note the tagging settings for ports (see table 39) that are part of a redundant Ring or the Ring/network coupling.

Redundancy	VLAN membership
HIPER-Ring	VLAN1 MU
MRP	any
Network/Ring coupling	VLAN1 MU

Table 39: Tagging settings of ports integrated into redundant Rings or the Ring/network coupling.

Note: In a redundant Ring with VLANs, you should only operate devices whose software version supports VLANs:

- RS2 xx/xx (from vers. 7.00),
- RS2-16M,
- RS 20, RS 30, RS 40 (with L2E, L2P)
- MICE (from rel. 3.0)
- Power MICE
- MS 20, MS 30
- RSR20, RSR30
- MACH 100
- MACH 1000
- MACH 4000
- MACH 3000 (from rel. 3.3)
- OCTOPUS

4.5.4 VLAN Port

With this dialog you can:

- assign ports to VLANs
- define the Acceptable Frame Type
- activate/deactivate Ingress Filtering

Parameter	Meaning	Value range	Default setting
Module	Module of the device on which the port is located.		
Port	Port to which this entry applies.		
Port VLAN ID	Specifies to which VLAN the port assigns a received untagged data packet.	All allowed VLAN IDs	1
Acceptable Frame Types	Specifies whether the port may also receive untagged data packets.	- admitAll - admitOnlyVlanTagged	admitAll
Ingress Filtering	Specifies whether the port evaluates the received tags.	on/off	off

Table 40: VLAN Port dialog

Note: Note the following:

- HIPER-Ring
  Select the port VLAN ID 1 for the Ring ports and deactivate “`Ingress Filtering`”.
- MRP-Ring
  - If the MRP-Ring configuration (see on page 109 „Configuring the MRP-Ring“) is not assigned to a VLAN, select the port VLAN ID 1.
  - If the MRP-Ring configuration (see on page 109 „Configuring the MRP-Ring“) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.
- Network/Ring coupling
  Select the VLAN ID 1 for the coupling and partner coupling ports and deactivate “`Ingress Filtering`”.

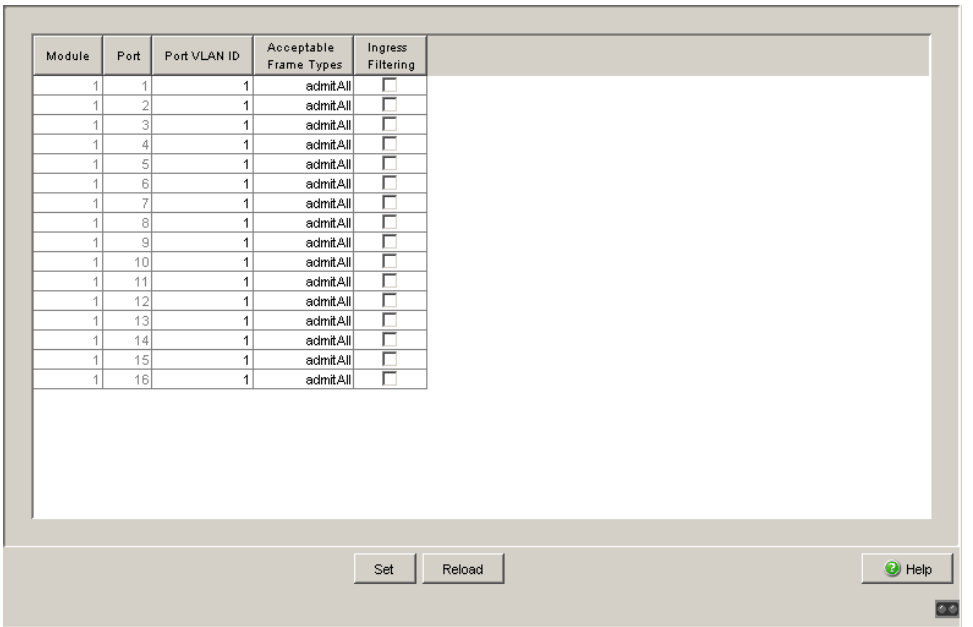


Figure 29: VLAN Port dialog

5 QoS/Priority

The device enables you to set

- how it evaluates the QoS/prioritizing information of incoming data packets:
  - VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
  - Type of Service (ToS) or DiffServ (DSCP) for IP packets (Layer 3)
- which QoS/prioritizing information it writes to outgoing data packets (e.g. priority for management packets, port priority).

The QoS/Priority menu contains the dialogs, displays and tables for configuring the QoS/priority settings:

- Global
- Port Configuration
- 802.1D/p Mapping
- IP DSCP mapping

5.1 Global

With this dialog you can:

- enter the VLAN priority for management packets in the range 0 to 7 (default setting: 0).
  In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
  In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.
  Note the assignment of the VLAN priority to the traffic class (see table 44).
- enter the IP-DSCP value for management packets in the range 0 to 63 (default setting: 0 (be/cs0)).
  In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
  In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.
  Note the assignment of the IP-DSCP value to the traffic class (see table 45).

  Note: Certain DSCP values have DSCP names, such as be/cs0 to cs7 (class selector) or af11 to af43 (assured forwarding) and ef (expedited forwarding).

- display the maximum number of queues possible per port.
  The device supports 4 (8 for MACH 4000 and PowerMICE) priority queues (traffic classes in compliance with IEEE 802.1D).
- select the trust mode globally. You use this to specify how the device handles received data packets that contain priority information.
  - “untrusted”
    The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
  - “trustDot1p”
    The device prioritizes received packets that contain VLAN tag information (assigning them to a traffic class - see „802.1D/p Mapping“).
    The device prioritizes received packets that do not contain any VLAN tag information (assigning them to a traffic class - see „Entering the port priority“) according to the port priority of the receiving port .

- “trustIpDscp”
  The device prioritizes received IP packets (assigning them to a traffic class - see „IP DSCP mapping“) according to their DSCP value.
  The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see „Entering the port priority“) according to the port priority of the receiving port .
  For received IP packets:
  The device also performs VLAN priority remarking.
  In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag (see on page 88 „VLAN Static“).
  Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with table 41.
  Example: Received IP packet with a DSCP value of 32 (cs4) is assigned to traffic class 2 (default setting). The packet was received at a port with port priority 2. Based on table 41, the VLAN priority is set to 4.

Traffic class	New VLAN priority when receiving port has an even port priority	New VLAN priority when receiving port has an odd port priority
0	0	1
1	2	3
2	4	5
3	6	7

Table 41: VLAN priority remarking

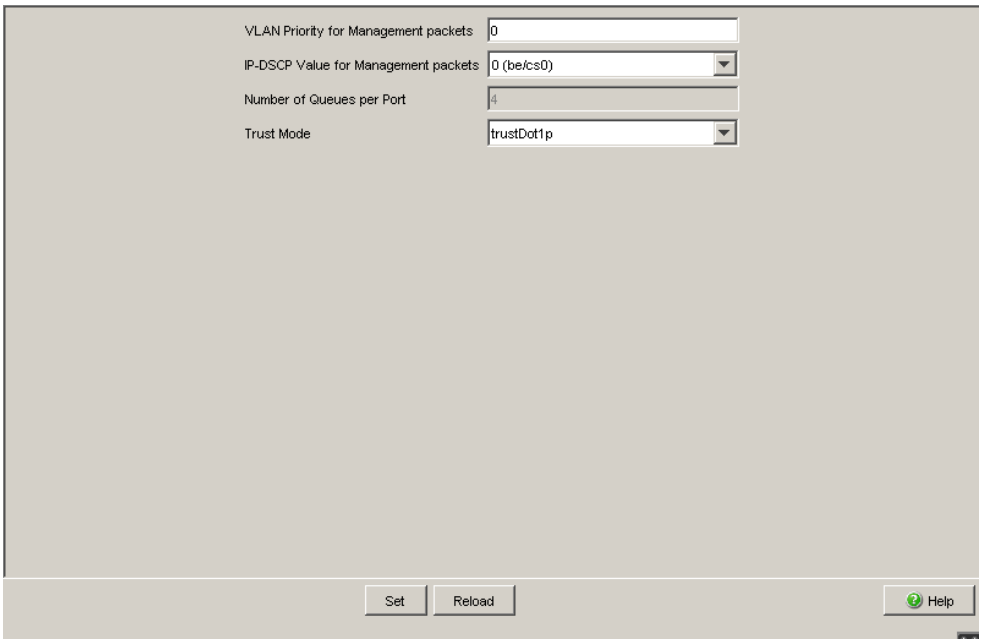


Figure 30: Global dialog

5.2 Port configuration

This dialog allows you to configure the ports. You can:

- assign a port priority to a port,

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port priority	Enter the port priority.

Table 42: Port configuration table

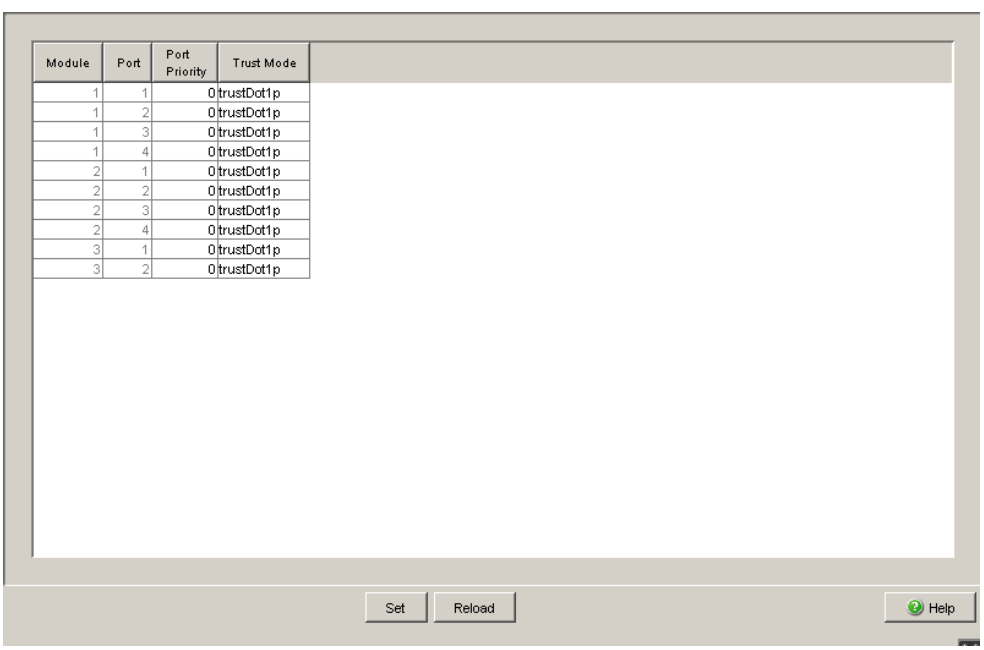


Figure 31: Port configuration dialog

5.2.1 Entering the port priority

☐ Double-click on a cell in the “Port priority” column and enter the priority (0-7).
According to the priority entered, the device assigns the data packets that it receives at this port to a traffic class (see table 43).
Prerequisite:
setting in the `Global:Trust Mode dialog: untrusted` (see on page 94 „Global“) or
setting in the `Global:Trust Mode dialog:trustDot1p` `Global:Trust Mode dialog: untrusted` (see on page 94 „Global“) and the data packets do not contain a VLAN tag or
setting in `Global:Trust Mode dialog: trustIpDscp` `Global:Trust Mode dialog: untrusted` (see on page 94 „Global“) and the data packets are not IP packets.

Port priority	Traffic class (default setting)	IEEE 802.1D traffic type
0	1	Best effort (default)
1	0	Background
2	0	Standard
3	1	Excellent effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, less than 100 milliseconds of latency and jitter
6	3	Voice, less than 10 milliseconds of latency and jitter
7	3	Network control reserved traffic

Table 43: Assigning the port priority to the four traffic classes

5.3 802.1D/p Mapping

The 802.1D/p mapping table allows you to assign a traffic class to every VLAN priority.

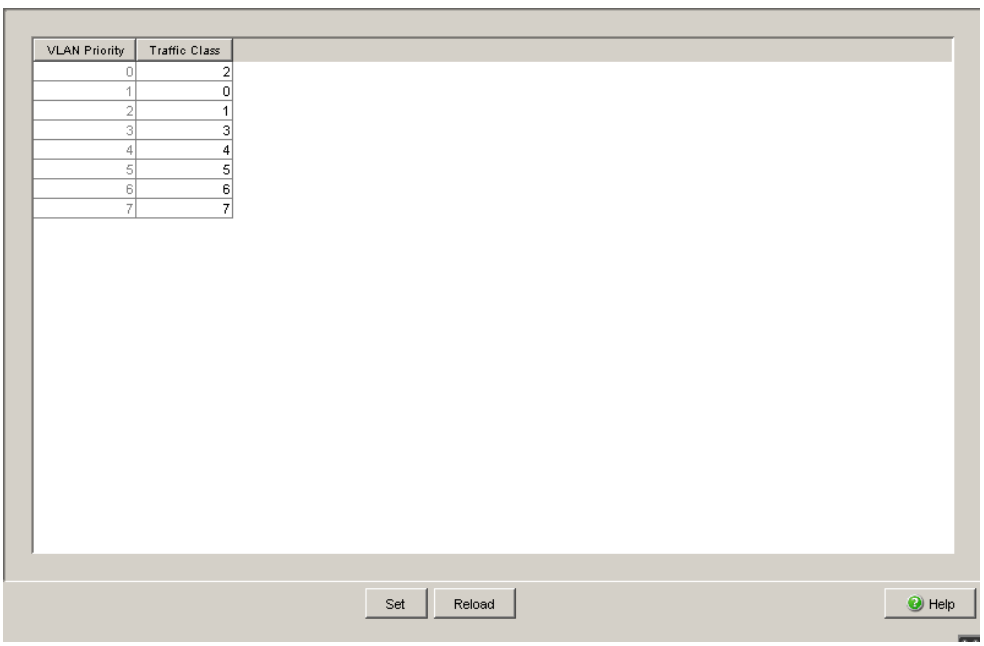


Figure 32: 802.1D/p mapping table

☐ Enter the desired value from 0 to 3 in the Traffic Class field for every VLAN priority.

VLAN priority	Traffic class (default setting)	IEEE 802.1D traffic type
0	1	Best effort (default)
1	0	Background
2	0	Standard
3	1	Excellent effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, less than 100 milliseconds of latency and jitter
6	3	Voice, less than 10 milliseconds of latency and jitter
7	3	Network control reserved traffic

Table 44: Assigning the VLAN priority to the four traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic class 3. Therefore, you select other traffic classes for application data.

5.4 IP DSCP mapping

The IP DSCP mapping table allows you to assign a traffic class to every DSCP value.

☐ Enter the desired value from 0 to 3 in the Traffic Class field for every DSCP value (0-63).

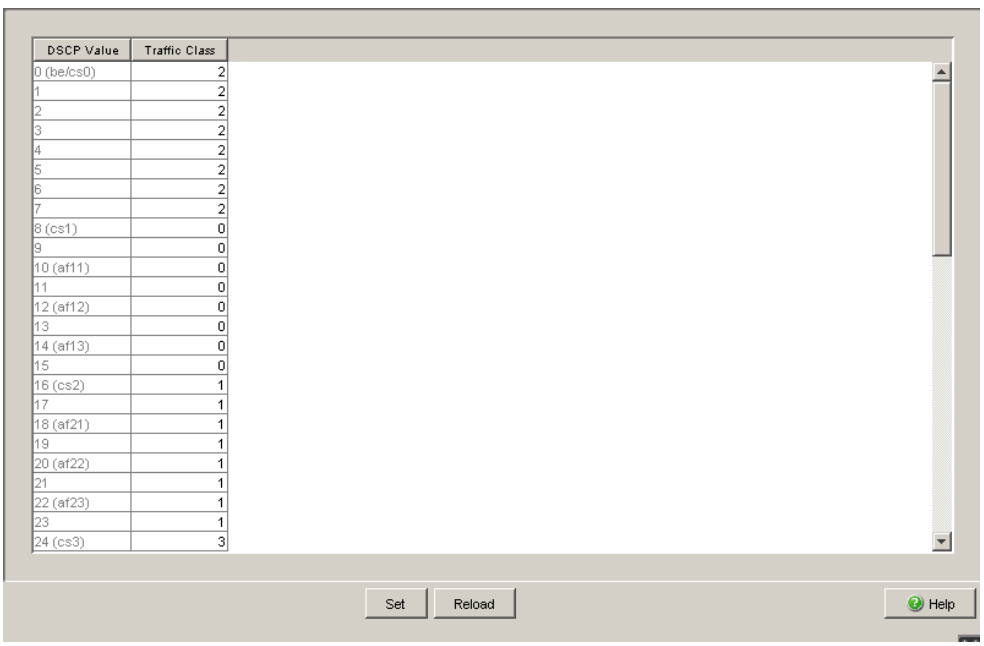


Figure 33: IP DSCP mapping table

The different DSCP values get the device to employ a different forwarding behavior, namely Per-Hop Behavior (PHB).
PHB classes:

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service.
  Reduced delay, jitter + packet loss (RFC 2598)
- Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC 2597).

- Default Forwarding/Best Effort: No particular prioritizing.

DSCP value	DSCP name	Traffic class (default setting)
0	Best Effort /CS0	1
1-7		1
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	0
17,19,21,23		0
18,20,22	AF21,AF22,AF23	0
24	CS3	1
25,27,29,31		1
26,28,30	AF31,AF32,AF33	1
32	CS4	2
33,35,37,39		2
34,36,38	AF41,AF42,AF43	2
40	CS5	2
41,42,43,44,45,47		2
46	EF	2
48	CS6	3
49-55		3
56	CS7	3
57-63		3

Table 45: Mapping the DSCP values onto the traffic classes

^

6 Redundancy

Under Redundancy you will find all the dialogs and views for configuring and monitoring the redundancy functions:

- Ring Redundancy
- Redundant coupling of Rings and network segments
- Rapid Spanning Tree Algorithm (RSTP)

6.1 Ring Redundancy

The concept of the Ring Redundancy enables the construction of high-availability, ring-shaped network structures.

If a section is down, the ring structure of a

- HIPER-(**HI**GH **PE**RFORMANCE **R**EDUNDANCY) Ring with up to 50 devices typically transforms back to a line structure within 80 ms (setting: standard/accelerated).
- MRP (**M**edia **R**edundancy **P**rotocol) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).

With the help of the **R**ing **M**anager (RM) function of a device, you can connect both ends of a backbone in a line structure to form a redundant ring.

With the help of the **R**ing **M**anager (RM) function of a device, you can connect both ends of a backbone in a line structure to form a redundant ring.

- Within a HIPER-Ring, you can use any combination of the following devices:
  - RS1
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - Power MICE
  - MACH 100
  - MACH 1000
  - MACH 3000
  - MACH 4000
- Within an MRP-Ring, you can use devices that support the MRP protocol based on IEC62439.
- Within a Fast HIPER-Ring, you can use any combination of the following devices:
  - RSR20, RSR30
  - MACH 1000

Depending on the device model, the Ring Redundancy dialog allows you to:

- Select one of the available Ring Redundancy versions, or change it.
- Display an overview of the current Ring Redundancy configuration.
- Create new Ring Redundancies.
- Configure existing Ring Redundancies.
- Enable/disable the Ring Manager function.
- Receive Ring information.
- Delete the Ring Redundancy.

Note: Enabled Ring Redundancy methods on a device are mutually exclusive at any one time. When changing to another Ring Redundancy method, deactivate the function for the time being.

Parameter	Meaning

Version	Select the Ring Redundancy version you want to use:
	`HIPER-Ring`
	`MRP`
	Default setting is HIPER-Ring

Ring port No.	In a ring, every device has 2 neighbors. Define 2 ports as ring ports to which the neighboring devices are connected.
Module	Module identifier of the ports used as ring ports
Port	Port identifier of the ports used as ring ports
Operation	Value depends on the Ring Redundancy version used. Described in the following sections for the corresponding Ring Redundancy version.

Table 46: Ring Redundancy basic configuration

6.1.1 Configuring the HIPER-Ring

For the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	off	on
Port	on	on
Duplex	Full	–

Table 47: Port settings for ring ports

Note: Configure all the devices of the HIPER-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the HIPER-Ring. You thus avoid loops during the configuration phase.

Note: As an alternative to using software to configure the HIPER-Ring, with devices RS20/30/40 and MS20/30 you can also use a DIP switch to enter a number of settings. You can also use a DIP switch to enter a setting for whether the configuration via DIP switch or the configuration via software has priority. The state on delivery is “Software Configuration”.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: `active`: This port is switched on and has a link. `inactive`: This port is switched off or it has no link.
Redundancy Manager Status (Ring Manager)	Status information, no input possible: `Active (redundant line)`: the redundant line was closed because a data line or a network component within the ring is down. `Inactive`: the redundant ring is open, and all data lines and network components are working.

Table 48: HIPER-Ring configuration

Parameter	Meaning
Ring Recovery	Select the desired value for the device for which you have activated the ring manager. If you have selected `Accelerated` for the ring recovery and the stability of the ring is not meeting your requirements for your network, then select `Standard`. **Note:** Settings in the “Ring Recovery” frame are only effective for devices that are ring managers.
Information	The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 48: HIPER-Ring configuration

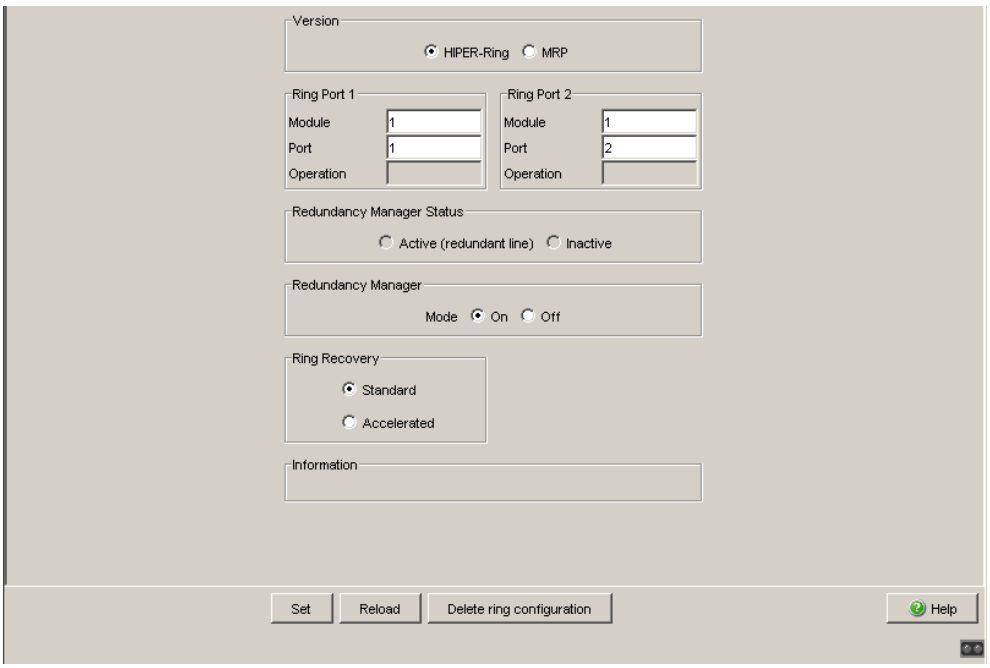


Figure 34: Selecting ring redundancy, entering ring ports, enabling/disabling ring manager and selecting ring recovery.

Note: Deactivate the Spanning Tree protocol for the ports connected to the redundant ring, because the Spanning Tree and the Ring Redundancy work with different reaction times (`Redundancy:Rapid Spanning Tree:Port`).
If you used the DIP switch to activate the HIPER-Ring function, RSTP is automatically switched off.

Note: If you have configured VLANS, note the VLAN configuration of the ring ports.
In the configuration of the HIPER-Ring, you select for the ring ports
– VLAN ID 1 and
– VLAN membership Untagged in the static VLAN table

Note: When you use the DIP switch to switch from a normal port to a ring port, the device makes the required settings for the pre-defined ring ports in the configuration table. The port which has been switched back from a ring port to a normal port keeps the ring port settings (transmission speed and mode). Independently of the DIP switch setting, you can still change all the ports via the software.

6.1.2 Configuring the MRP-Ring

To configure an MRP-Ring, you set up the network to meet your requirements. For the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	off	on
Port	on	on
Duplex	Full	–

Table 49: Port settings for ring ports

Note: Configure all the devices of the MRP-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the MRP-Ring. You thus avoid loops during the configuration phase.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: `forwarding`: This port is switched on and has a link. `blocked`: This port is blocked and has a link. `disabled`: This port is switched off. `not connected`: This port has no link.
Configuration Redundancy Manager (Ring Manager)	Deactivate the advanced mode if a device in the ring does not support the advanced mode for fast switching times. Otherwise you activate the advanced mode. **Note:** All Hirschmann devices that support the MRP-Ring also support the advanced mode.
Operation	When you have configured all the parameters for the MRP-Ring, you switch the operation on here. When you have configured all the devices in the MRP-Ring, you close redundant lines.
Ring Recovery	Select the desired value for the device for which you have activated the ring manager. Select 500 ms for the ring recovery if the ring stability does not meet the requirements of your network. `Note`: Settings in the “Ring Recovery” frame are ineffective for devices that are not ring managers.

Table 50: MRP-Ring configuration

Parameter	Meaning
VLAN ID	If you have configured VLANs, you select `VLAN ID 0` here if you do not want to assign the MRP-Ring configuration to a VLAN. Note the VLAN configuration of the ring ports: Select for VLAN ID 1 and VLAN membership U in the static VLAN table for the ring ports. `VLAN ID > 0` if you want to assign the MRP-Ring configuration to this VLAN. Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring. Note the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership T in the static VLAN table.
Information	The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 50: MRP-Ring configuration

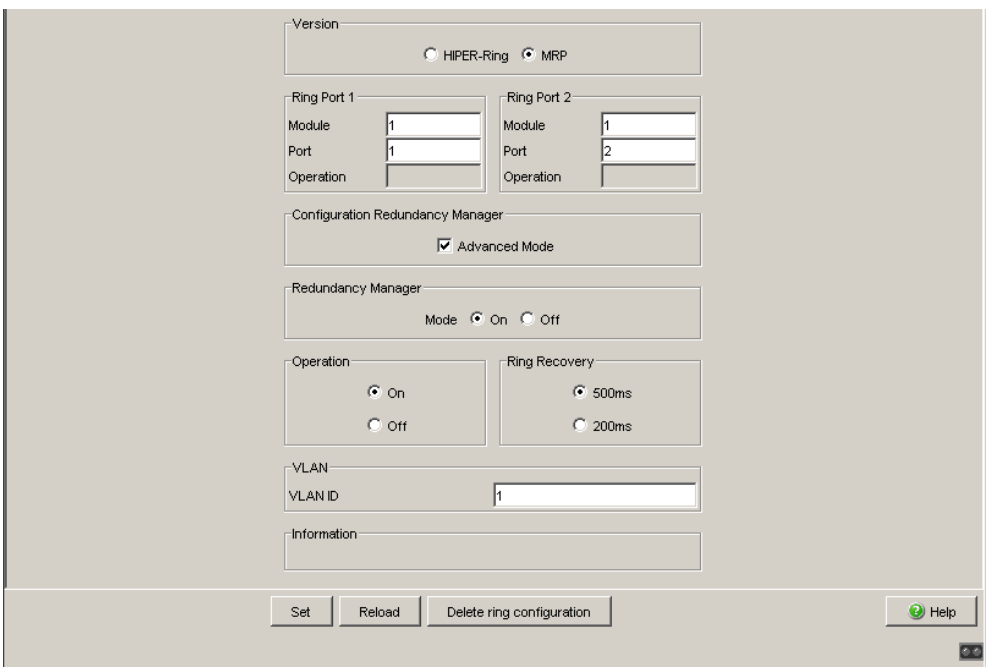


Figure 35: Selecting MRP-Ring version, entering ring ports and enabling/disabling ring manager

Note: Activate the MRP compatibility (Rapid Spanning Tree:Global) on all devices in a MRP-Ring if you want to use RSTP in the MRP-Ring. If this is not possible, e.g, because several devices do not support MRP compatibility, deactivate the Spannung Tree Protocol on the ports connected to the MRP-Ring. Spanning Tree and Ring redundancy affect each other.
If you combine RSTP with a MRP-Ring, take care to configure the bridges in the MRP-Ring with a better RSTP bridge priority than those in the connected RSTP network. Thus you avoid connection interruptions in case the devices in the MRP-Ring detect a failure and shut down.

6.2 Ring/Network coupling

With this dialog you can:
- display an overview of the existing Ring/Network coupling,
- configure a Ring/Network coupling,
- switch a Ring/Network coupling on/off,
- create a new Ring/Network coupling, and
- Delete Ring/Network couplings

6.2.1 Preparing a Ring/Network coupling

STAND-BY switch

The devices have a STAND-BY switch, with which you can define the role of the device within a Ring/Network coupling.
Depending on the device, this switch is a DIP switch or a software switch (`Redundancy:Ring/Network Coupling` dialog). By setting this switch, you define whether the device has the main coupling or the redundant coupling within a Ring/Network coupling.

Note: Depending on the model, the devices have a DIP switch, with which you can choose between the software configuration and the DIP switch configuration. If the software configuration is set, the other DIP switches have no effect.

Device type	STAND-BY switch type
RS2-./.	DIP switch
RS2-16M	DIP switch
RS20/RS30/RS40	Can be switched between DIP switch and software switch
MICE/Power MICE	Can be switched between DIP switch and software switch
MS20/MS30	Can be switched between DIP switch and software switch
OCTOPUS	Software switch
MACH 100	Software switch
MACH 3000/MACH 4000	Software switch

Table 51: Overview of the STAND-BY switch types

Depending on the device and model, set the STAND-BY switch in accordance with the following table (see table 52):

Device with	Choice of main coupling or redundant coupling
DIP switch	On “STAND-BY” DIP switch
DIP switch/software switch option	According to the option selected - on “STAND-BY” DIP switch or in the - `Redundancy:Ring/Network Coupling` dialog, by making selection in “Select configuration”. **Note:** These devices have a DIP switch, with which you can choose between the software configuration and the DIP switch configuration. If you have set the software configuration, changing the other DIP switches has no effect.
Software switch	In the `Redundancy:Ring/Network Coupling` dialog

Table 52: Setting the STAND-BY switch

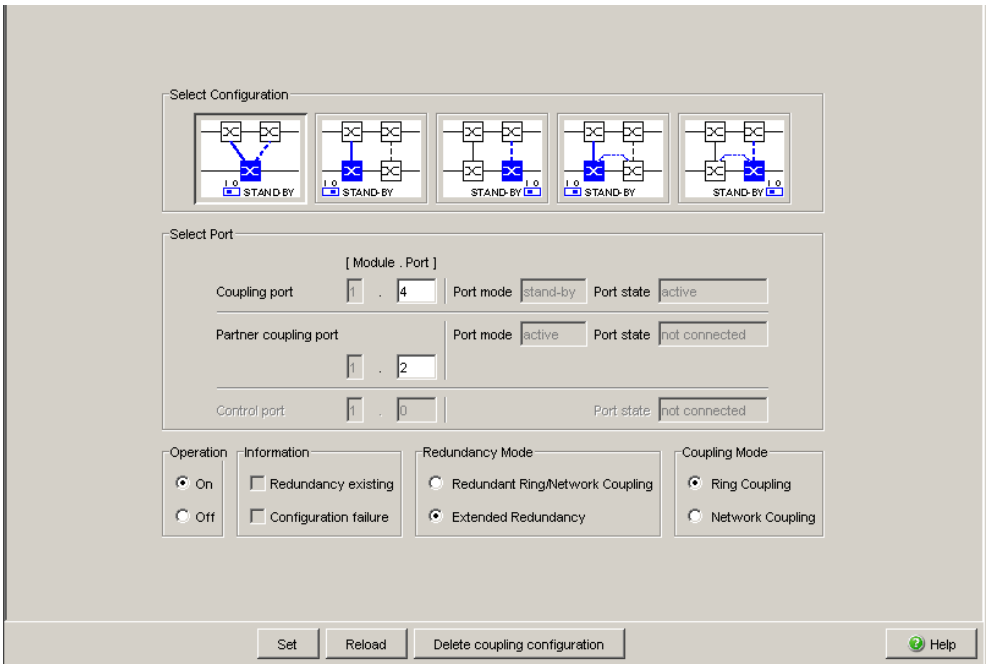


Figure 36: Software configuration of the STAND-BY switch

Depending on the STAND-BY DIP switch position, the dialog displays those configurations that are not possible in gray. If you want to select one of these grayed-out configurations, you put the STAND-BY DIP switch on the Switch into the other position.

One-Switch coupling
Assign the device the DIP switch setting “STAND-BY”, or use the software configuration to assign the redundancy function to it.

Two-Switch coupling
Assign the device in the redundant line the DIP switch setting “STAND-BY”, or use the software configuration to assign the redundancy function to it.

Note: For redundancy security reasons, the combination of Rapid Spanning Tree and Ring/Network Coupling is not possible.

Ring/Network Coupling dialog

Parameter	Meaning
Selecting the configuration	Depending on your local conditions, select “One-Switch coupling”, “Two-Switch coupling” or “Two-Switch coupling with control line”. You use the STAND-BY switch to select whether there is a main connection or a redundant connection. If you have made settings via the DIP switch, you cannot overwrite them via the software, and constellations that cannot be selected are grayed-out. Select the relevant Ring/Network coupling constellation by selecting the corresponding symbol.
Coupling port	This is the port to which you have connected a redundant connection. **Note:** Configure the coupling port and the ring ports, if there are any ring ports, on different ports. **Note:** To avoid continuous loops, the device sets the port status of the coupling port to “off” if you switch off the function or change the configuration while the connections are operating at these ports.
Port mode	- `active` You have switched the port on. - `stand-by` The port is in stand-by mode.
Port state	- `active`: You have switched the port on. - `stand-by`: The port is in stand-by mode. - `not connected`: You have not connected the port.
Partner coupling port	This is the port at which the partner has made its connection. It is only possible or necessary to enter a port here if “One-Switch coupling” is being set up. **Note:** Configure the partner coupling port and the ring ports, if there are any ring ports, on different ports.
IP Address	If you have selected “Two-Switch coupling”, the IP address of the partner is displayed here if you have already started operating the partner in the network.
Control port	This is the port to which you connect the control line.
Operation	Here you switch the Ring/Network coupling for this device on or off
Information	The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 53: Ring/Network Coupling dialog

Parameter	Meaning
Redundancy Mode	With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. Both lines are never active simultaneously. With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if the connection line between the devices in the connected network fails. During the reconfiguration period, package duplications may possibly occur. Therefore, only select this setting if your application detects package duplications.
Coupling Mode	Here you define whether the constellation you are configuring is a coupling of redundancy rings (HIPER-Ring, MRP-Ring or Fast HIPER-Ring), or network segments. Here you define whether the constellation you are configuring is a coupling of redundancy rings (HIPER-Ring, MRP-Ring), or network segments.

Table 53: Ring/Network Coupling dialog

The following tables show the selection options and default settings for the ports used in the Ring/Network coupling.

Device	Partner coupling port	Coupling port
RS2-./.	Not possible	Not possible
RS2-16M	All ports (default setting: port 2)	All ports (default setting: port 1)
RS20, RS30, RS40	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
OCTOPUS	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MICE	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
Power MICE	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MS20	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MS30	All ports (default setting: port 2.3)	All ports (default setting: port 2.4)
RSR20/30	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MACH 100	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MACH 1000	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MACH 3000	All ports	All ports
MACH 4000	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)

Table 54: Port assignment for one-Switch coupling

Device	Coupling port
RS2-./.	Not possible
RS2-16M	Adjustable for all ports (default setting: port 1)
RS20, RS30, RS40	Adjustable for all ports (default setting: port 1.4)
OCTOPUS	Adjustable for all ports (default setting: port 1.4)
MICE	Adjustable for all ports (default setting: port 1.4)
Power MICE	Adjustable for all ports (default setting: port 1.4)
MS20	Adjustable for all ports (default setting: port 1.4)
MS30	Adjustable for all ports (default setting: port 2.4)
RSR20/30	Adjustable for all ports (default setting: port 1.4)
MACH 100	Adjustable for all ports (default setting: port 1.4)
MACH 1000	Adjustable for all ports (default setting: port 1.4)
MACH 3000	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)

Table 55: Port assignment for the redundant coupling (two-Switch coupling)

Device	Coupling port	Control port
RS2-./.	Port 1	Stand-by port (can only be combined with RS2-../..)
RS2-16M	Adjustable for all ports (default setting: port 1)	Adjustable for all ports (default setting: port 2)
RS20, RS30, RS40	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
OCTOPUS	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.4)
MICE	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
Power MICE	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MS20	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MS30	Adjustable for all ports (default setting: port 2.4)	Adjustable for all ports (default setting: port 2.3)
RSR20/RSR30	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 100	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 1000	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 3000	Adjustable for all ports	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)

Table 56: Port assignment for the redundant coupling (two-Switch coupling with control line)

Note: For the coupling ports, select the following settings in the `Basic Settings:Port Configuration` dialog:
– Port: on
– Automatic configuration (autonegotiation):
on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX
for glass fiber connections

Note: If you have configured VLANS, note the VLAN configuration of the coupling and partner coupling ports.
In the Ring/Network Coupling configuration, select for the coupling and partner coupling ports
– VLAN ID 1 and "`Ingress Filtering`" disabled in the port table and
– VLAN membership `MU` in the static VLAN table.

Note: If you are operating the Ring Manager and two-Switch coupling functions at the same time, there is the risk of creating a loop.

6.3 Rapid Spanning Tree

With this dialog you can:
- switch the Rapid Spanning Tree Protocol on/off.,
- view device-specific information on the Rapid Spanning Tree Protocol,
- configure device-specific parameters of the Rapid Spanning Tree Protocol, and
- configure port-specific parameters of the Rapid Spanning Tree Protocol.

Note: The Spanning Tree and Rapid Spanning Tree protocols based on IEEE 802.1D-2004 and IEEE 802.1w respectively are protocols for MAC bridges. For this reason, the following description of these protocols usually employs the term bridge instead of switch.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it usually makes sense to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus the total failure of the network. To prevent this, the (Rapid) Spanning Tree Algorithm was developed. The Rapid Spanning Tree Protocol (RSTP) enables redundancy by interrupting loops.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge fails, the STP requires a maximum of 30 seconds to reconfigure. This was no longer acceptable in time-sensitive applications. The STP was therefore developed to the RSTP, leading to average reconfiguration times of less than a second. If you use RSTP in a ring topology with 10 - 20 devices, you can achieve reconfiguration times in the range of milliseconds.

Note: RSTP resolves a given topology to a tree structure (Spanning Tree). The number of devices in a branch (from the root to the branch tip) is limited by the parameter Max Age. The default value for Max Age is 20, it can be increased to 40.
You should note the following here: If the root device fails and another device takes over the root function, the largest possible number of devices decreases accordingly.
When network segments are connected to a MRP ring and you enable MRP compatibility, a peculiarity results. If the root bridge is located inside the MRP ring, the devices inside the MRP ring are combined into one virtual device for the purpose of calculating the branch length.

Note: When coupling network segments to a MRP-Ring and activating the MRP compatibility, there is a modification. If the root bridge is located in the MRP-Ring, the devices inside the MRP-Ring are combined into one virtual device when calculating the segment length.

Note: The RSTP Standard dictates that all the devices within a network work with the (Rapid) Spanning Tree Algorithm. However, if STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost. RSTP devices also work in a limited MSTP environment within the scope of their functionality.

Note: Due to a change in the IEEE 802.1D-2004 standard on which RSTP is based, the Standards Commission has reduced the maximum value for the “Hello Time” from 10 to 2. When earlier firmware versions are upgraded to version 5.x or higher, the firmware automatically changes a locally entered “Hello Time” value greater than 2 to 2.
If the device is not the RSTP root, “Hello Time” values greater than 2 can remain valid, depending on the firmware version of the root device.

6.3.1 Rapid Spanning Tree Global

Note: Rapid Spanning Tree is enabled by default on all devices and autonomously begins to resolve the discovered topology to a tree structure. If you disable RSTP on certain devices, avoid loops during the configuration phase.

Parameter	Meaning	Value range	Default setting
Operation	Switch the RSTP function for this device „On” or „Off”. If you disable RSTP globally on a device, it will flood the RSTP frames like normal multicast frames. The device behaves transparently regarding RSTP frames.	On, Off	
MRP-Kompat-ibilität	MRP compatibility facilitates the use of RSTP in a MRP-Ring and when coupling RSTP segments to a MRP-Ring, on the condition that all devices in the MRP-Ring support the MRP compatibility. If you combine RSTP with a MRP-Ring, take care to configure the bridges in the MRP-Ring with a better RSTP bridge priority than those in the connected RSTP network. Thus you avoid connection interruptions in case the devices in the MRP-Ring detect a failure and shut down.	On, Off	Off
Root Information	In every RSTP environment, there is a root Switch that is responsible for controlling the RSTP function. The parameters of the current root Switch are displayed here. – Root Id: Displays the bridge identifier of the root Switch. This is made up of the priority value and the MAC address of the device. “This device is root”: A checkmark shows that the device is currently the root Switch. – Root Port: Displays the port that leads to the root Switch. If you have configured the device itself as the root Switch, 0.0 is displayed. – Root Cost: Displays the root costs to the root Switch. If you have configured the device itself as the root Switch, 0 is displayed for the costs.		
Priority	The priority and MAC address together make up the device's bridge identification. The device with the lowest bridge identification becomes the root device. Define the root device by assigning the device the lowest priority in the bridge identification among all the devices in the network. Note that only multiples of 4,096 can be entered for this value.	0 < n*4,096 < 61,440	32,768

Table 57: Global RSTP settings
a: Note the connection between the parameters Forward Delay and Max Age - see below.

Parameter	Meaning	Value range	Default setting
Hello Time	The left column shows the value currently being used by the root bridge. The device periodically receives configuration frames (Hello frames) from the root bridge. The Hello Time shows the time between two successive configuration frames sent by the root bridge. If you configure the current device as the root bridge, the other devices in the entire network will assume the value in the right column.	1 - 2	2
Forward Delay	The left column shows the value currently being used by the root bridge. The predecessor protocol STP used the parameter to control (delay) the transition time between the states „disabled“, „blocking“, „learning“, ?„forwarding“. Since the introduction of RSTP, this parameter has only secondary relevance because state transitions are negotiated between RSTP bridges without a given time delay. If you configure the current device as the root bridge, the other devices in the entire network will assume the value in the right column.	4 - 30 (see a:)	30
Max Age	The left column shows the value currently being used by the root Switch. Contrary to the past (STP) meaning, Max Age now (for RSTP) denotes the maximum permissible branch length (number of devices to the root bridge). If you configure the current device as the root bridge, the other devices in the entire network will assume the value in the right column.	6 - 40 (see a:)	6
MAC Address	The MAC address is combined with the priority to make up the device's bridge identification.		
Topology Changes	This field displays the number of changes since RSTP started.		

Table 57: Global RSTP settings
a: Note the connection between the parameters Forward Delay and Max Age - see below.

Parameter	Meaning	Value range	Default setting
Time since last change	This field displays the time that has elapsed since the last network reconfiguration.		
Information	This frame shows if there is a configuration conflict. In this case, a device exists outside the MRP ring with the given MAC address. This device's displayed priority is better (numerically lower) than the root bridge's priority inside the MRP ring. To resolve the conflict, set the the displayed device's priority to a worse value (numerically higher) than root bridge's priority inside the MRP ring.		

Table 57: Global RSTP settings
a: Note the connection between the parameters Forward Delay and Max Age - see below.

The parameters
– Forward Delay and
– Max Age
have the following relationship to each other:

Forward Delay >= (Max Age/2) + 1

If you enter values that contradict this relationship, the device then replaces these values with a default value or with the last valid values.

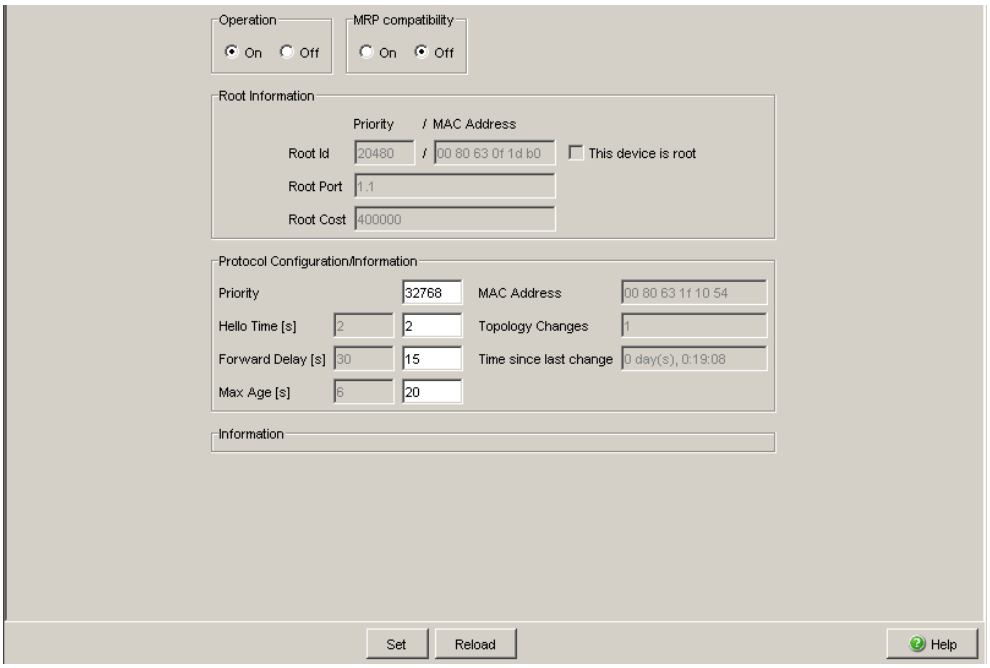


Figure 37: RSTP Global dialog

6.3.2 Rapid Spanning Tree Port

Note: Deactivate the Spanning Tree protocol on the ports connected to a HIPER-Ring or a Fast HIPER-Ring, because the Spanning Tree and the Ring Redundancy affect each other. Turn on the MRP compatibility in a MRP ring if you want to use RSTP and MRP.
If you combine RSTP with a MRP ring, take care that the bridges in the MRP ring have a better RSTP bridge priority than those in the connected RSTP network. Thus you avoid an connection interruption if devices in the MRP ring should fail.

Parameter	Meaning	Value range	Default setting
STP State Enable	Here you can turn RSTP on or off for this port. If you turn RSTP off for this port while RSTP is globally enabled for the device, the device will discard RSTP frames received on this port.	on, off	on
Port State	Displays the port state	disabled, forwarding, discarding, blocking, learning	-
Priority	Here you enter the first byte of the port identification.	16 < n*16 < 240	128
Port Path Cost	Enter the path costs to indicate preference for redundant paths. If the value is “0”, the Switch automatically calculates the path costs depending on the transmission rate.	0 - 200.000.000	0
Admin Edge Port	If the parameter is set to „true“, the port will transition to the forwarding state. If the port nevertheless receives a RSTP frame, it will transition to the blocking state and the bridge will then determine the new port role. .If the parameter’s value is „false“, the port remains in the blocked state until the bridge has determined the port role. Only after that will the port transition to its final state.	true, false	false
Oper Edge Port	Is „true“ if no RSTP frames were received, i. e., a terminal device that sends no RSTP frames is connected to this port. Is „false“ if RSTP frames were received, i. e., no terminal device but a bridge is connected.	true, false	-
Auto Edge Port	The setting for Auto Edge Port only takes effect if the parameter Oper Edge Port has been set to „false“. if Auto Edge Port is set to „true“, the port will transition to the forwarding state within 1.5 * Hello Time (3 seconds). If is is set to „false“, it will take 30 seconds until the edge port forwards data frames.	true, false	false

Table 58: Port-related RSTP settings and displays

Parameter	Meaning	Value range	Default setting
Oper Point-ToPoint	If this port has a full-duplex link to another RSTP device, the value for Oper PointToPoint will become „true“, else it will become „false“ (e. g., if a hub is connected). A Point-to-point connection is a direct connection between two RSTP devices. The direct, local communications between the two switches results in a short reconfiguration time.	true, false	auto (is calculated): FDX = true HDX = false
Designated Root	Displays the bridge identification of the designated root Switch for this port.	Bridge identification (hexadecimal)	-
Designated Costs	Display of the costs of the path from this port to the root Switch.	Costs	-
Designated Port	Display of the port identifier of the port that creates the connection to the root Switch for this port (on the designated Switch).	Port identification (hexadecimal) and port number	-

Table 58: Port-related RSTP settings and displays

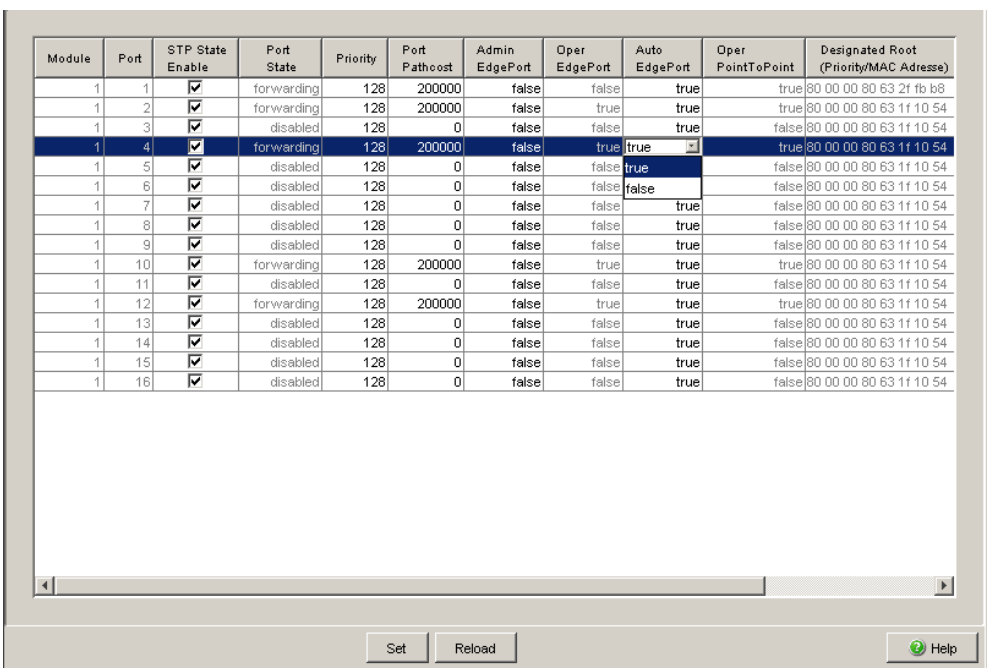


Figure 38: RSTP Port dialog

7 Diagnosis

The diagnosis menu contains the following tables and dialogs:

- Event Log
- Ports (statistics, utilization, SFP modules)
- Topology Discovery
- Port Mirroring
- Device Status
- Signal Contact
- Alarms (Traps)
- Report (log file, system information)
- IP Address Conflict Detection
- Self Test
- Service Mode

In service situations, they provide the technician with the necessary information for diagnosis.

7.1 Event log

The table under Event Log lists all the events with a time stamp.
The "Delete" button allows you to delete the contents of the Event Log window.

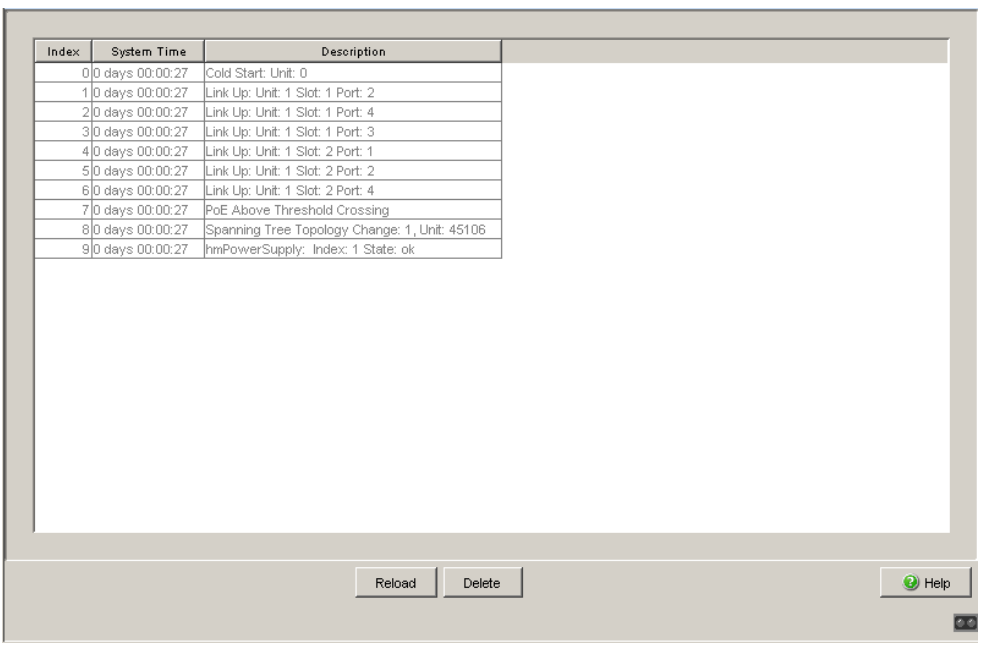

Index
System Time
Description
0 0 days 00:00:27 Cold Start: Unit: 0
1 0 days 00:00:27 Link Up: Unit: 1 Slot: 1 Port: 2
2 0 days 00:00:27 Link Up: Unit: 1 Slot: 1 Port: 4
3 0 days 00:00:27 Link Up: Unit: 1 Slot: 1 Port: 3
4 0 days 00:00:27 Link Up: Unit: 1 Slot: 2 Port: 1
5 0 days 00:00:27 Link Up: Unit: 1 Slot: 2 Port: 2
6 0 days 00:00:27 Link Up: Unit: 1 Slot: 2 Port: 4
7 0 days 00:00:27 PoE Above Threshold Crossing
8 0 days 00:00:27 Spanning Tree Topology Change: 1, Unit: 45106
9 0 days 00:00:27 hmPowerSupply: Index: 1 State: ok
Reload
Delete
Help

Figure 39: Event log table

7.2 Ports

The port menu contains displays and tables for the individual ports:

- Statistics table
- Utilization
- SFP Modules

7.2.1 Statistics table

This table shows you the contents of various event counters. In the Restart menu item, you can reset all the event counters to zero using "Warm start", "Cold start" or "Reset port counter".
The packet counters add up the events sent and the events received.

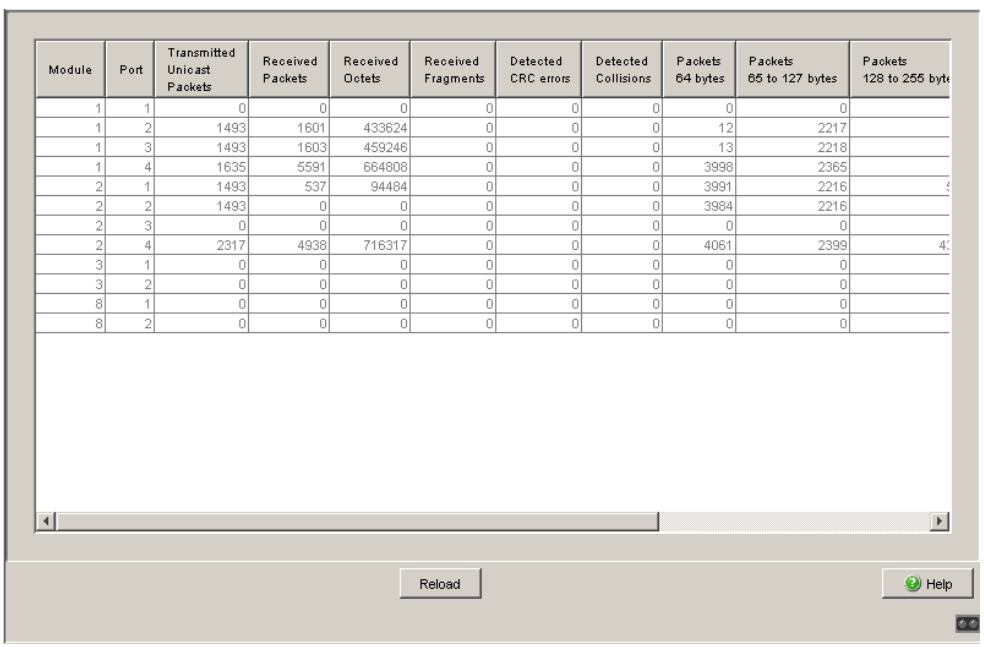


Figure 40: Port statistics table

7.2.2 Utilization

This table displays the network load of the individual ports.
In the “Upper Threshold[%]” column you enter the top threshold value for network load. If this threshold value is exceeded, the device sets a check mark in the “Alarm” field.
In the “Upper Threshold [%]” column you enter the lower threshold value for network load. If this threshold value is not met, the device removes the check mark previously set.

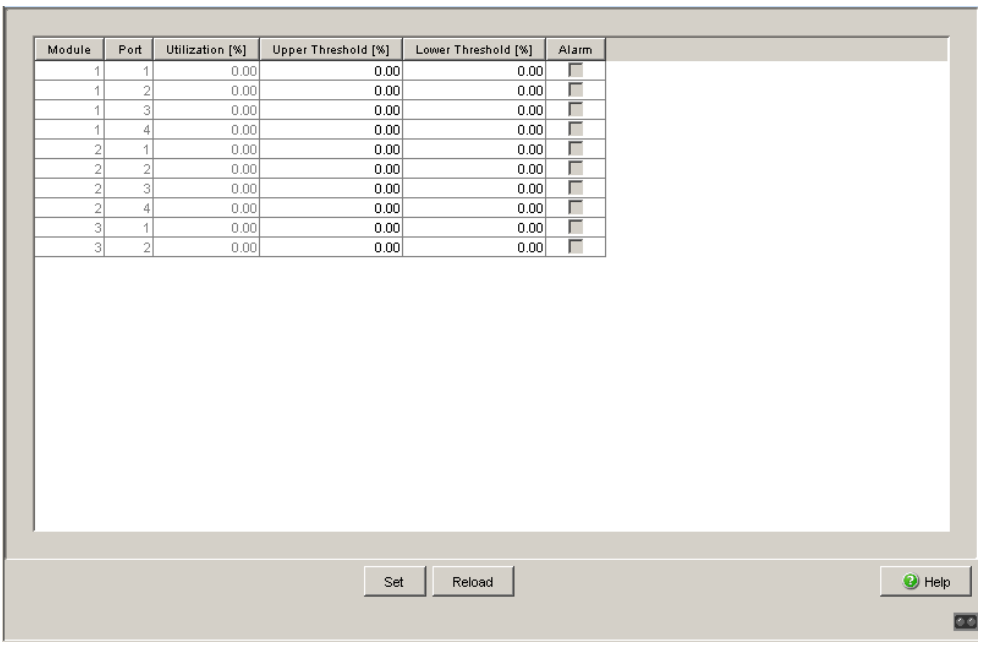


Figure 41: Network load dialog

7.2.3 SFP modules

The SFP status display allows you to look at the current SFP module connections and their properties. The properties include:

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Module type	Type of SFP module, e.g. M-SFP-SX/LC
Supported	Shows whether the media module supports the SFP module.
Temperature in Celsius	Shows the operating temperature of the SFP
Tx Power in mW	Shows the transmission power in mW
Rx Power in mW	Shows the receiver power in mW
Receiver power status	Shows the power level of the received signal. – good receiver power – limited receiver power – insufficient receiver power

Table 59: SFP Modules dialog

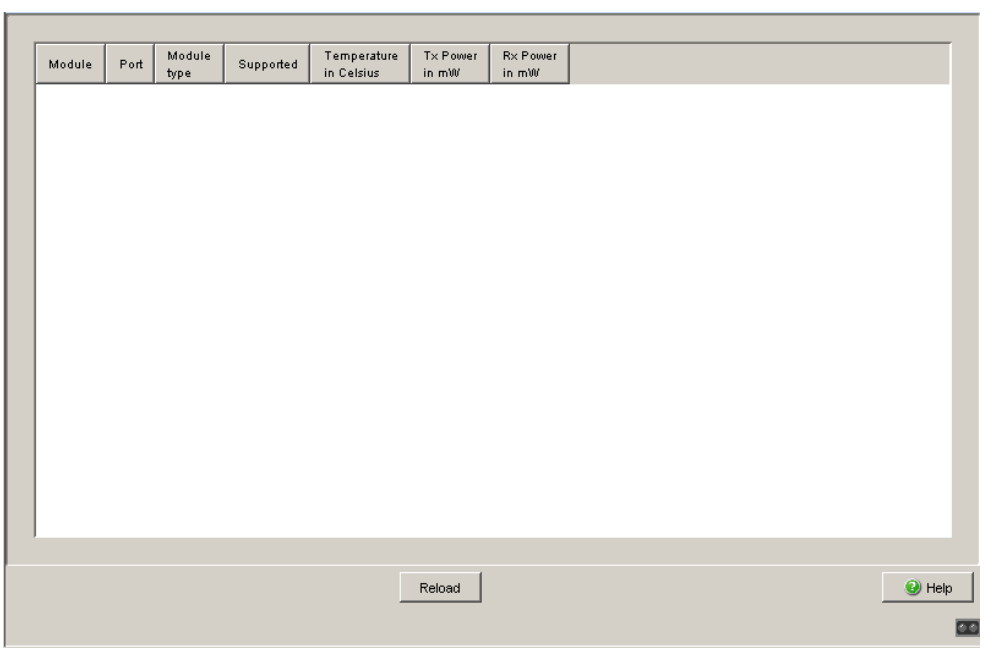


Figure 42: SFP Modules dialog

7.3 Topology Discovery

This dialog allows you to switch on/off the topology discovery function (LLDP). The topology table shows you the collected information for neighboring devices. This information enables the network management station to map the structure of your network.

The option "Show LLDP entries exclusively" allows you to reduce the number of table entries. In this case, the topology table hides entries from devices without active LLDP support.

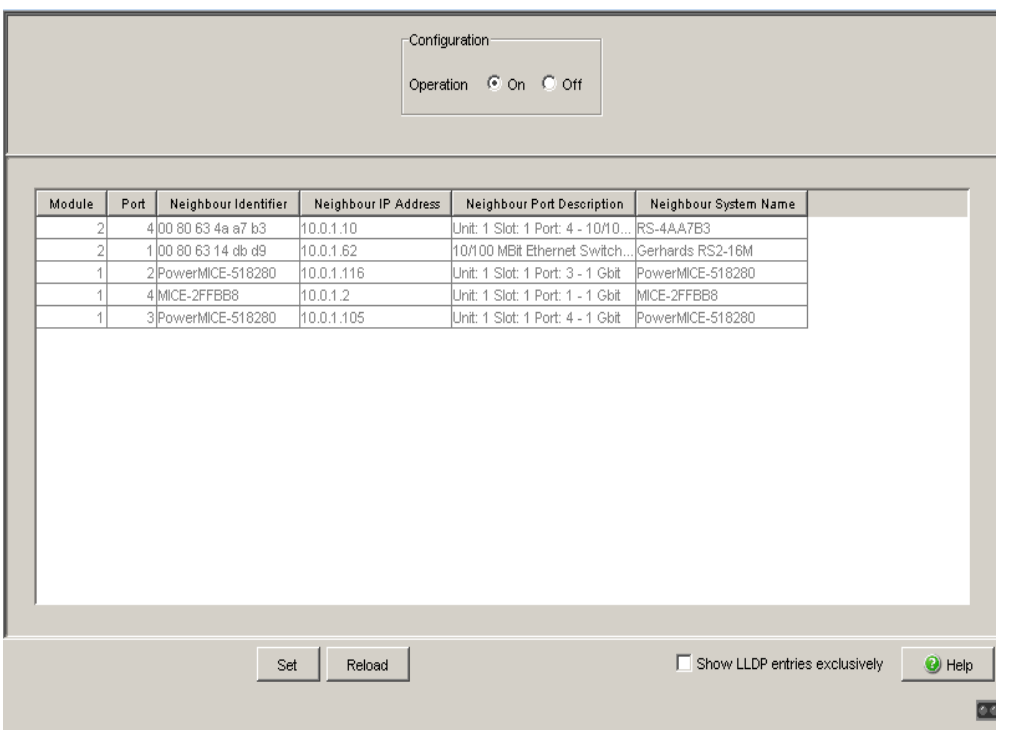

Configuration
Operation
On
Off
Module
Port
Neighbour Identifier
Neighbour IP Address
Neighbour Port Description
Neighbour System Name
2 4 00 80 63 4a a7 b3 10.0.1.10 Unit: 1 Slot: 1 Port: 4 - 10/10... RS-4A,A7B3
2 1 00 80 63 14 db d9 10.0.1.62 10/100 MBit Ethernet Switch... Gerhards RS2-16M
1 2 PowerMICE-518280 10.0.1.116 Unit: 1 Slot: 1 Port: 3 - 1 Gbit PowerMICE-518280
1 4 MICE-2FFBB8 10.0.1.2 Unit: 1 Slot: 1 Port: 1 - 1 Gbit MICE-2FFBB8
1 3 PowerMICE-518280 10.0.1.105 Unit: 1 Slot: 1 Port: 4 - 1 Gbit PowerMICE-518280
Set
Reload
Show LLDP entries exclusively
Help

Figure 43: Topology discovery

If several devices are connected to one port, for example via a hub, the table will contain one line for each connected device.

If

- devices with active topology discovery function and

- devices without active topology discovery function
  are connected to a port, the topology table hides the devices without active topology discovery.

If

- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices
  MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), (see on page 71 „Filters for MAC addresses“).

7.4 Port Mirroring

This dialog allows you to configure and activate the port mirroring function of the device.
In port mirroring, the valid data packets of one port, the source port, are copied to another, the destination port. The data traffic at the source port is not influenced by port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the source port's data traffic in sending and receiving direction.
The destination port forwards the data to be sent and blocks data received.

☐ Select the source port whose data traffic you want to observe.

☐ Select the destination port to which you have connected your management tool.

☐ Select "enabled" to switch on the function.

The "Delete" button in the dialog allows you to reset all the port mirroring settings of the device to the state on delivery.

Note: In active port mirroring, the specified port is used solely for observation purposes.

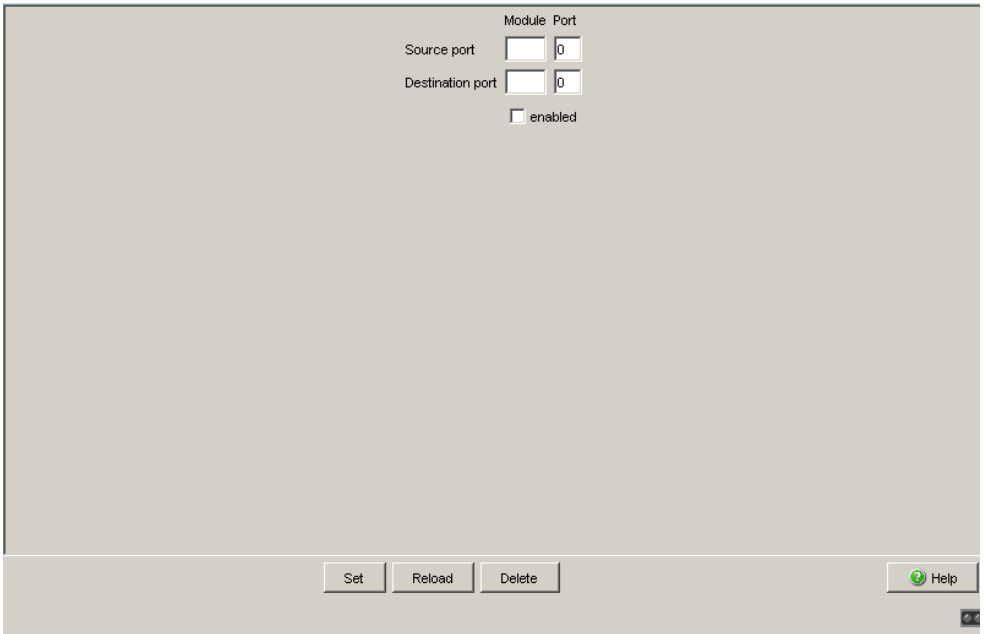


Figure 44: Port Mirroring dialog

7.5 Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

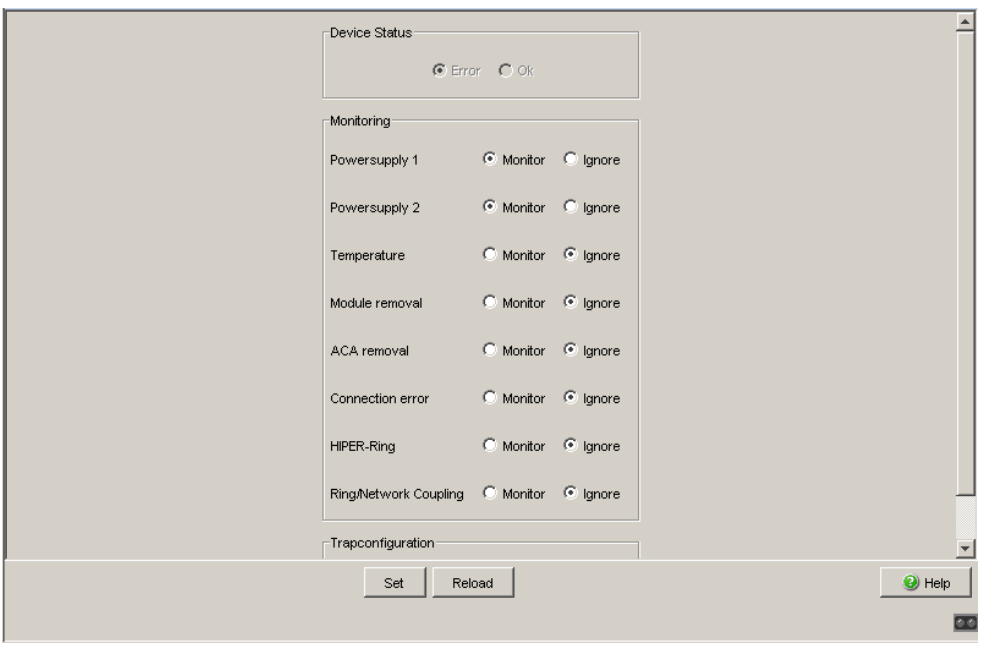


Figure 45: Device State dialog (for power MICE)

☐ In the "Monitoring" field, you select the events you want to monitor.
☐ To monitor the temperature, you set the temperature thresholds in the `Basics:System` dialog at the end of the system data.

The events which can be selected are:

Name	Meaning
Power supply ...	Monitor/ignore supply voltage(s).
Temperature	Monitor/ignore temperature thresholds set (see on page 16 „System“) for temperatures that are too high/too low
Module removal	Monitor/ignore the removal of a module (for modular devices).
ACA removal	Monitor/ignore the removal of the ACA.
Connection error	Monitor/ignore the defective link status of at least one port. The reporting of the link status can be masked for each port by the management (see on page 25 „Port configuration“). Link status is not monitored in the state on delivery.
HIPER-Ring	Monitor/ignore the discard of the existing redundancy (in Ring Manager mode). State on delivery: ring redundancy is not monitored.
Ring/Network Coupling	Monitor/ignore the failure of the redundancy. State on delivery: ring redundancy is not monitored. The following conditions are also reported by the device in standby mode: – Defective link status of the control line – Partner device is in standby mode.
Fan	Monitor/ignore fan function (for devices with fan).

Table 60: Device Status

☐ Select "Generate Trap" in the "Trap configuration" field to activate the sending of a trap if the device state changes.

Note: With non-redundant voltage supply, the device reports the absence of a supply voltage. You can prevent this message by feeding the supply voltage over both inputs, or by switching off the monitoring (see on page 140 „Signal contact“).

7.6 Signal contact

The signal contacts are used for

- controlling external devices by manually setting the signal contacts,
- monitoring the functions of the device,
- reporting the device state of the device.

7.6.1 Manual setting

☐ Select the tab page "Alarm 1" or "Alarm 2" (for devices with two signal contacts).
☐ In the "Signal contact mode" field, you select the "Manual setting" mode. With this mode you can control this signal contact remotely.
☐ Select "Opened" in the "Manual setting" frame to open the contact.
☐ Select "Closed" in the "Manual setting" frame to close the contact.

Application options:

- Simulation of an error during SPS error monitoring.
- Remote control of a device via SNMP, such as switching on a camera.

7.6.2 Function monitoring

☐ Select the tab page “Signal contact 1” or “Signal contact 2” (for devices with two signal contacts).

☐ In the “Mode Signal contact” field, you select the “Monitoring correct operation” mode. In this mode the signal contacts monitor the functions of the device, thus enabling remote diagnosis.
A break in contact is reported via the potential-free signal contact (relay contact, closed circuit):

- Voltage supply 1/2 failure or continuous device malfunction (internal voltage). Select “Monitor” for the power supply if the signal contact should report the failure of the voltage supply or the internal 3.3 VDC voltage.
- The temperature threshold has been exceeded or has not been reached (see on page 17 „System data“). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).
- Fan failure (for devices with a fan).
- The removal of the ACA. Select “Monitor” for ACA removal if the signal contact is to report the removal of an ACA (for devices which support the ACA).
- The defective link status of at least one port. The reporting of the link status can be masked via the management for each port in the device. Link status is not monitored in the state on delivery. Select “Monitor” for connection errors if the signal contact is to report a defective link status for at least one port.
- Redundancy failure in the redundant ring (see on page 104 „Ring Redundancy“). Select “Monitor” for the ring redundancy if the signal contact is to report a redundancy that no longer exists in the redundant ring.
- Error in the Ring/Network coupling. Select “Monitor” for the Ring/Network coupling if the signal contact is to report an error in the Ring/Network coupling (see on page 112 „Preparing a Ring/Network coupling“).

In RM mode, the device also signals the following state:

- Redundancy existing. State on delivery: ring redundancy is not monitored.

7.6.3 Device status

☐ Select the tab page “Alarm 1” or “Alarm 2” (for devices with two signal contacts).
☐ In the “Mode Signal Contact” field, you select the “Device status” mode. In this mode, the signal contact is used to monitor the status of the device (see on page 138 „Device Status“) and thereby makes remote diagnosis possible.
The device status “Error” (see on page 138 „Device Status“) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

7.6.4 Configuring traps

☐ Select `generate Trap`, if the device is to create a trap as soon as the position of a signal contact changes when function monitoring is active.

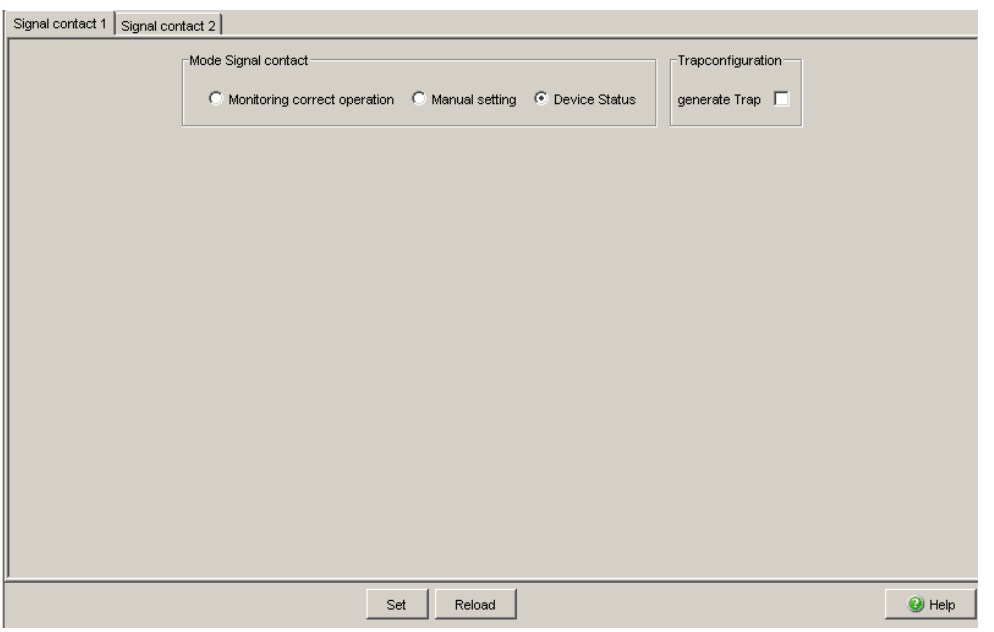


Figure 46: Signal contact dialog

7.7 Alarms (Traps)

This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

☐ Select „Create entry“.
☐ In the „Address“ column, enter the IP address of the management station to which the traps should be sent.
☐ In the „Enabled“ column, you mark the entries which should be taken into account when traps are being sent.
☐ In the „Selection“ frame, select the trap categories from which you want to send traps.

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt, (see on page 40 „SNMPv1/v2 Access Settings“), (see on page 136 „Port Mirroring“).
Link Up/Down	At one port of the device, the link to a device connected there has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: – The status of a supply voltage has changed (see the System dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. – A media module was added or removed. – The AutoConfiguration AdapterACA was added or removed. – The temperature threshold was exceeded/not reached. – The receiver power status of a port with an SFP module has changed (see dialog `Dialog:Ports:SFP Modules`).
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or the redundant Ring/Network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 61: Trap categories

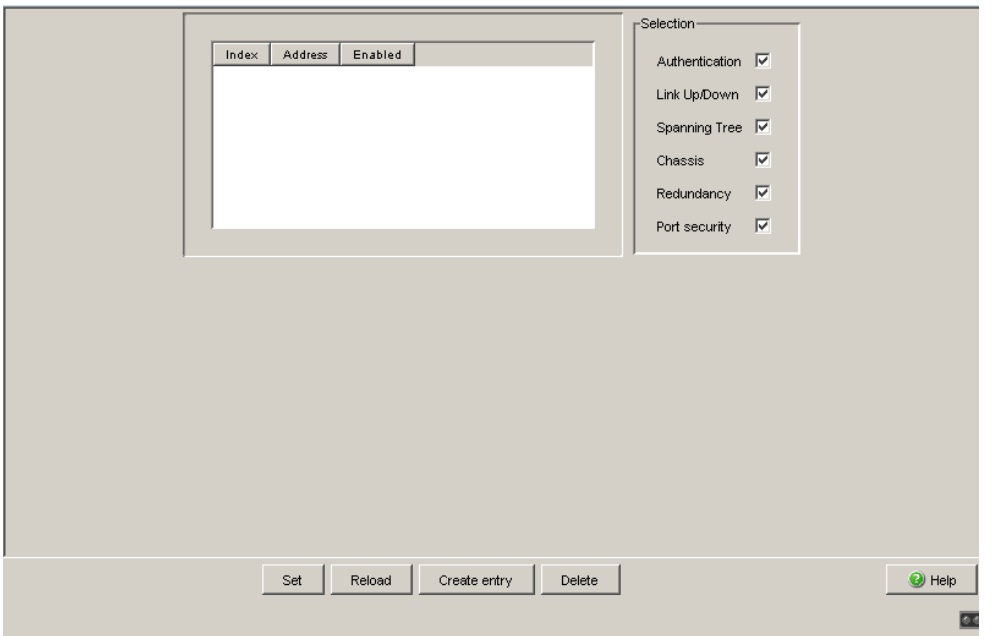


Figure 47: Alarms dialog

7.8 Report

The following reports are available for the diagnostics:

- Log file.
  The log file is an HTML file in which the device writes all the important device-internal events.
- System information.
  The system information is an HTML file containing all system-relevant data.
- Security Data Sheet IAONA.
  The security data sheet IAONA is a data sheet in the XML format that has been standardized by IAONA (Industrial Automation Open Networking Alliance). Among other data, it contains security-related information on the accessible ports and the associated protocols.

7.9 IP address conflict detection

This dialog allows you to detect address conflicts the device is having with its own IP address and rectify them (Address Conflict Detection, ACD).

☐ Select IP address conflict detection on/off under “Status” or select the mode (see table 62).

Mode	Meaning
enable	Enables active and passive detection.
disable	Disables the function
activeDetectionOnly	Enables active detection only. After connecting to a network or after an IP address has been configured, the device immediately checks whether its IP address already exists within the network. If the IP address already exists, the device will return to the previous configuration, if possible, and make another attempt after 15 seconds. This prevents the device from connecting to the network with a duplicate IP address.
passiveOnly	Enables passive detection only. The device listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network.

Table 62: Possible address conflict operation modes

▶ In the table the device logs IP address conflicts with its IP address.
For each conflict the device logs:
  ▶ the time
  ▶ the conflicting IP address
  ▶ the MAC address of the device with which the IP address conflicted.

For each IP address, the device logs a line with the last conflict that occurred.

☐ You can delete this table by restarting the device.

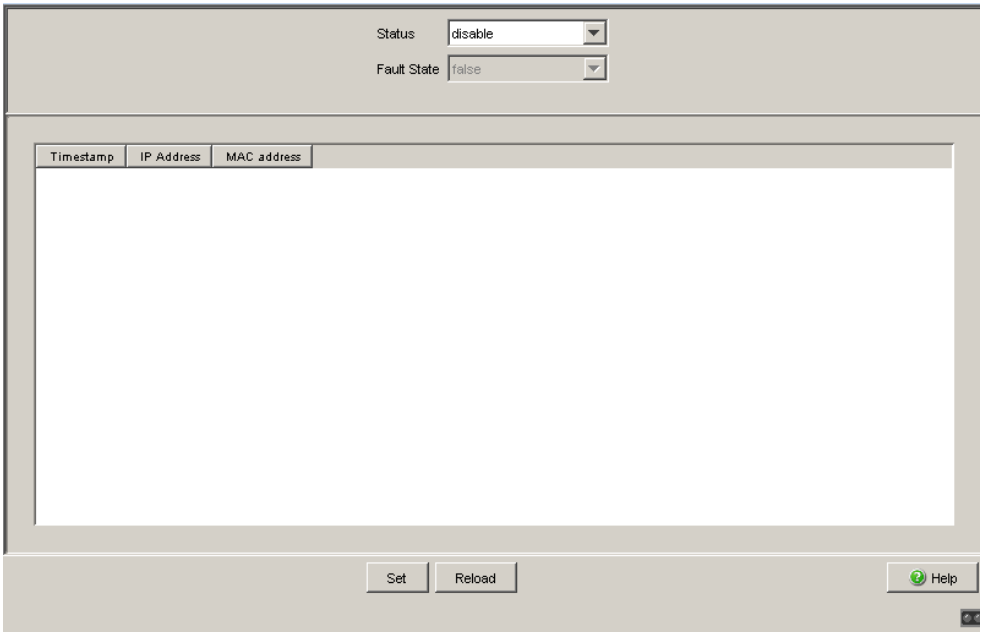


Figure 48: IP Address Conflict Detection dialog

7.10Self Test

With this dialog you can:

- activate/deactivate the RAM test for a cold start of the device. Deactivating the RAM test shortens the booting time for a cold start of the device.
- allow or prevent a restart due to an undefined software state.

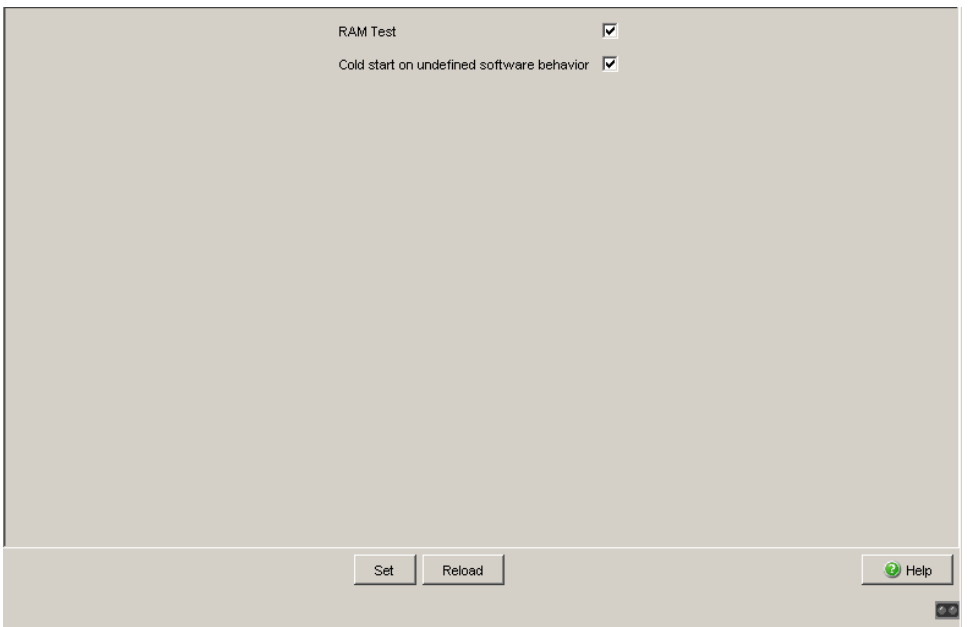


Figure 49: Self-test dialog

7.11 Service mode

The service mode enables you to divide the device into two transmission areas. You can thus, for example, perform test or service configurations in the field area of a network while the ongoing operation continues in the backbone area.

The device determines the two transmission areas via the HIPER-Ring ports: transmission area 1 only includes the HIPER-Ring ports of the device, while all other ports belong to transmission area 2. When the service mode is activated, the device creates a new VLAN in which all the ports of transmission area 2 are members. You use the redundant supply voltage (see below) to activate the service mode. You can view the configuration of the newly created VLAN in the dialogs under Switching/VLAN, but the device does not allow these entries to be changed, in order to keep the service configuration. By generating the VLAN, the device

- resets the port VLAN IDs for all the ports of this VLAN to the new VLAN ID
- deactivates GVRP at all ports of this VLAN. The device thus prevents GVRP from dynamically changing the service mode port settings.
- activates “ingress filtering” at all ports of this VLAN. Thus the device only transmits packets when the input and output ports belong to this VLAN.

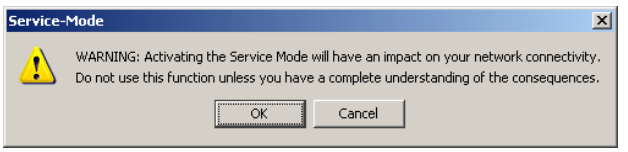
7.11.1 Activating the service mode

Prerequisites:

– HIPER-Ring ports are defined (HIPER-Ring or MRP-Ring).
– The supply voltage is redundant at P1 and P2.

Note: If there is no redundant voltage when the service mode is being activated (by clicking on “Set” - see below), the Switch immediately creates the two transmission areas. Depending on the settings already entered, this can break your link to the Switch.

☐ Select the `Diagnostics:Service Mode` dialog.
☐ Activate “Mode”.
☐ Enter a number not equal to 0 or 1 in the “VLAN” field. Enter a VLAN ID for a new VLAN in order to keep the settings for existing VLANs.
☐ Click on “Set”. The device outputs the following warning:


Service-Mode
WARNING: Activating the Service Mode will have an impact on your network connectivity.
Do not use this function unless you have a complete understanding of the consequences.
OK
Cancel

☐ It you are sure that your link to the Switch will not be broken, click on “OK” to activate the service mode.

The device will indicate in all dialogs that the service mode is activated.

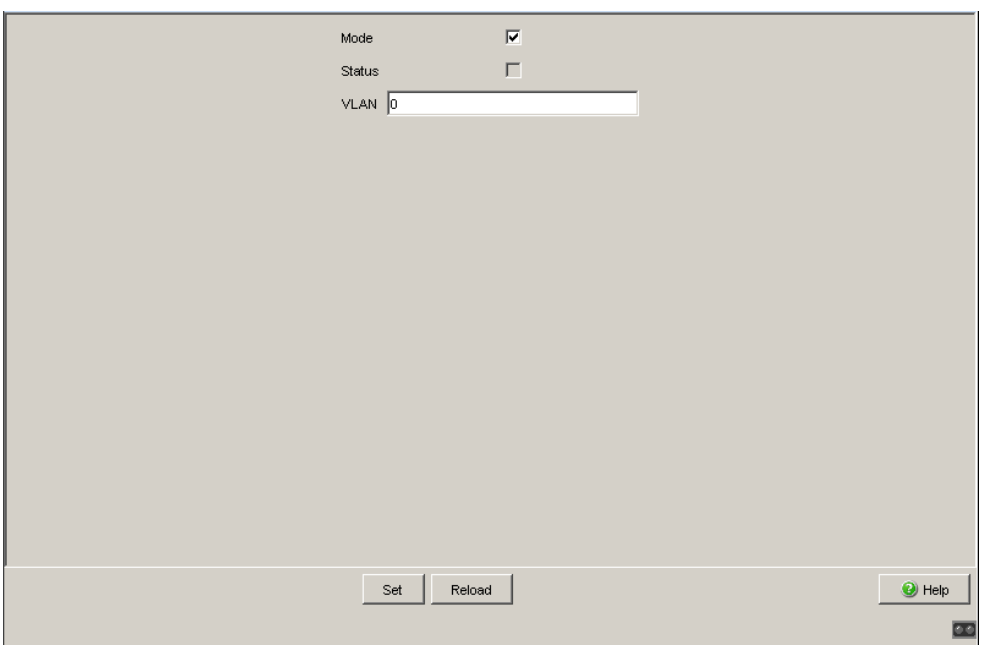


Figure 50: Service Mode dialog - mode activated

☐ Deactivate the redundant supply voltage.

The service mode is now activated, which the device indicates with a checkmark in the “Status” field.

Note: Deactivate the service mode (see below) when saving the device configuration (dialog: `Basics:Load/Save:Save:On the Switch`).

7.11.2 Deactivating the service mode

☐ Reactivate the redundant voltage.

The service mode is now deactivated.

☐ Select the `Diagnostics:Service Mode` dialog.
☐ Deactivate “Mode”.
☐ Click on “Set” to deactivate the service mode.
This prevents the device from switching to the service mode if the redundant voltage supply fails.

Note: After the service mode is deactivated, the device takes on its previous settings again.

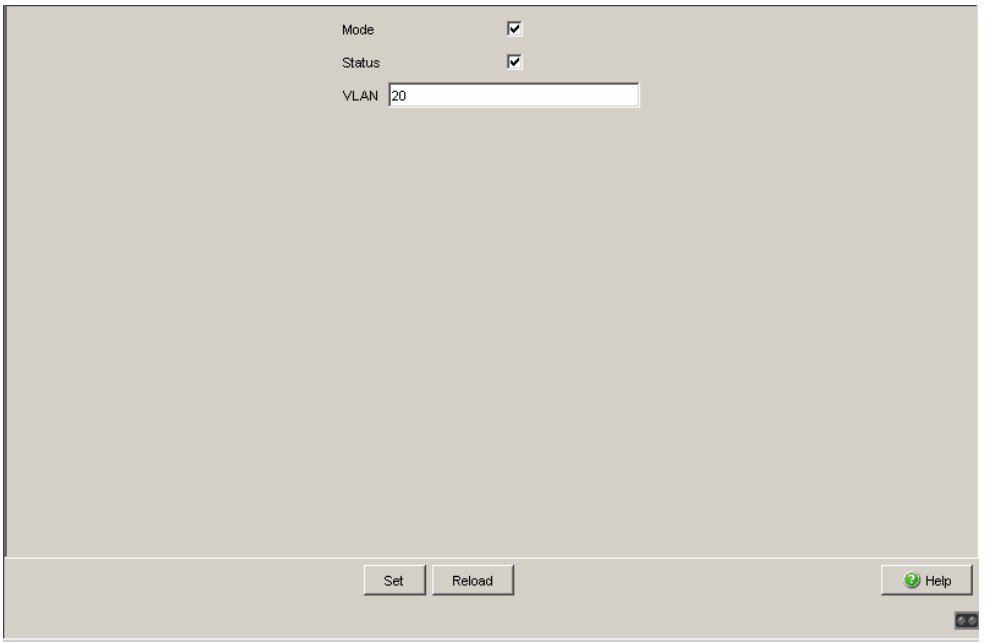


Figure 51: Service Mode dialog - mode deactivated

8 Advanced

The menu contains the dialogs, displays and tables for:

- DHCP Relay Agent
- Industry Protocols
- Command Line

8.1 DHCP Relay Agent

This dialog allows you to configure the DHCP relay agent.

☐ Enter the DHCP server IP address.
If one DHCP server is not available, then you can enter up to three additional DHCP server IP addresses, so that the device can change to another DHCP server.

☐ With Option 82, a DHCP relay agent which receives a DHCP request adds an “Option 82” field to the request, as long as the request received does not already have such a field.
When the function is switched off, the device will forward attached “Option 82” fields, but it will not add any on. Under “Type”, you specify the format in which the device recognition of this device is entered in the “Option 82” field by the DHCP relay agent.
The options are:
– IP Address
– MAC Address (state on delivery)
– System name (client ID)
– Other (freely definable ID, which you can specify in the following rows).
“DHCP server RemoteID entry” shows you the value that you enter when configuring your DHCP server. “Type display” shows the device recognition in the selected form.

▶ The “Circuit ID” column shows you the value which you enter when configuring your DHCP server. The “Circuit ID” contains the port number and the ID of the VLAN from which the DHCP has been received.

Example of a configuration of your DHCP server:
Type: `mac`
DHCP server for RemoteID entry: `00 06 00 80 63 00 06 1E`
Circuit ID: `B3 06 00 00 01 00 01 01`
This results in the entry for the “Hardware address” in the DHCP server:
`B30600000100010100060080630006 1E`

☐ In the “Option 82 on” column, you can switch this function on/off for each port.

☐ In the “Hirschmann Device” column, you mark the ports to which a Hirschmann device is connected.

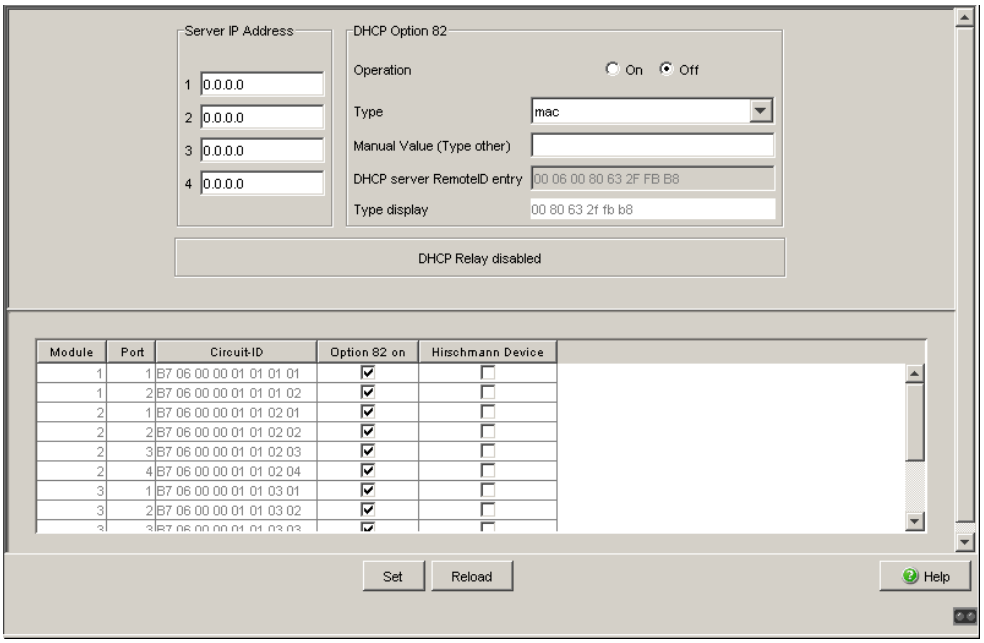

Server IP Address
1 0.0.0.0
2 0.0.0.0
3 0.0.0.0
4 0.0.0.0
DHCP Option 82
Operation
On
Off
Type
mac
Manual Value (Type other)
DHCP server RemoteID entry
00 06 00 80 63 2F FB B8
Type display
00 80 63 2f fb b8
DHCP Relay disabled
Module
Port
Circuit-ID
Option 82 on
Hirschmann Device
1 1 B7 06 00 00 01 01 01 01
1 2 B7 06 00 00 01 01 01 02
2 1 B7 06 00 00 01 01 02 01
2 2 B7 06 00 00 01 01 02 02
2 3 B7 06 00 00 01 01 02 03
2 4 B7 06 00 00 01 01 02 04
3 1 B7 06 00 00 01 01 03 01
3 2 B7 06 00 00 01 01 03 02
Set
Reload
Help

Figure 52: DHCP Relay Agent dialog

8.2 Industrial Protocols

With this dialog you can:

- activate and deactivate the PROFINET IO or EtherNet/IP industrial protocols
- download the GSDML/EDS file for configuring the PLC of this device to your PC.
- download the GSDML/EDS file for configuring the PLC of another device to your PC. The input field allows you to define the other device
  - by selecting a device from a list or
  - by entering the product code

Detailed information on industrial protocols and PLC configuration is contained in the User Manual „Industrial Protocols“.

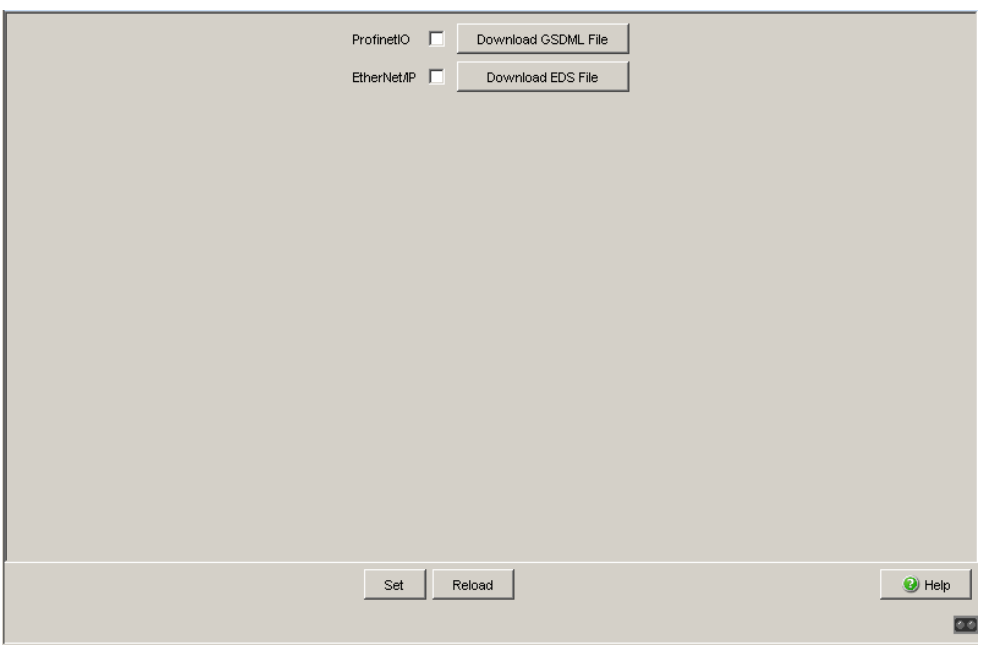


Figure 53: Industry Protocols dialog

8.2.1 PROFINET IO

To integrate this into a control system,
☐ activate the function in the "ProfinetIO" frame
☐ click on "Download GSDML File" to load the GSDML file onto your PC
☐ in the `Basic Settings:Network` dialog, check whether `Local` is selected in the "Mode" frame (see on page 21 „Network“),
☐ in the `Switching:VLAN:Global` dialog, check whether "VLAN 0 Transparent Mode" is selected (see on page 83 „VLAN Global“),
☐ configure the alarm settings and the threshold values for the alarms you want to monitor (see on page 138 „Device Status“),
☐ configure the SPS as described in the "Industry Protocols" user manual

8.2.2 EtherNet/IP

To integrate this into a control system,
☐ activate the function in the "EtherNet/IP" frame
☐ click on "Download EDS File" to load the EDS file onto your PC
☐ in the `Switching: Multicasts` dialog, check whether IGMP Snooping is activated (see on page 75 „Multicasts“),
☐ configure the SPS as described in the "Industry Protocols" user manual

8.3 Command Line

This window enables you to access the Command Line Interface (CLI) using the Web interface.

You will find detailed information on CLI in the “Command Line Interface” reference manual.

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	8000
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable via GMRP/IGMP Snooping	512
Max. length of over-long packets (from 03.0.00)	1632

VLAN	
VLAN ID	1 to 4042
Number of VLANs	max. 255 simultaneously per device max. 255 simultaneously per port
Number of VLANs in GMRP in VLAN 1	max. 255 simultaneously per device max. 255 simultaneously per port

A.2 List of RFCs

RFC 768	(UDP)
RFC 783	(TFTP)
RFC 791	(IP)
RFC 792	(ICMP)
RFC 793	(TCP)
RFC 826	(ARP)
RFC 854	(Telnet)
RFC 855	(Telnet Option)
RFC 951	(BOOTP)
RFC 1112	(IGMPv1)
RFC 1157	(SNMPv1)
RFC 1155	(SMIv1)
RFC 1212	(Concise MIB Definitions)
RFC 1213	(MIB2)
RFC 1493	(Dot1d)
RFC 1542	(BOOTP-Extensions)
RFC 1643	(Ethernet-like -MIB)
RFC 1757	(RMON)
RFC 1769	(SNTP)
RFC 1867	(HTML/2.0 Forms w/ file upload extensions)
RFC 1901	(Community based SNMP v2)
RFC 1905	(Protocol Operations for SNMP v2)
RFC 1906	(Transport Mappings for SNMP v2)
RFC 1907	(Management Information Base for SNMP v2)
RFC 1908	(Coexistence between SNMP v1 and SNMP v2)
RFC 1945	(HTTP/1.0)
RFC 2068	(HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
RFC 2131	(DHCP)
RFC 2132	(DHCP-Options)
RFC 2233	(The Interfaces Group MIB using SMI v2)
RFC 2236	(IGMPv2)
RFC 2246	(The TLS Protocol, Version 1.0)
RFC 2271	(SNMP Framework MIB)
RFC 2346	(AES Ciphersuites for Transport Layer Security)
RFC 2365	(Administratively Scoped Boundaries)
RFC 2570	(Introduction to SNMP v3)
RFC 2571	(Architecture for Describing SNMP Management Frameworks)
RFC 2572	(Message Processing and Dispatching for SNMP)
RFC 2573	(SNMP v3 Applications)
RFC 2574	(User Based Security Model for SNMP v3)

RFC 2575	(View Based Access Control Model for SNMP)
RFC 2576	(Coexistence between SNMP v1, v2 & v3)
RFC 2578	(SMI v2)
RFC 2579	(Textual Conventions for SMI v2)
RFC 2580	(Conformance statements for SMI v2)
RFC 2613	(SMON)
RFC 2618	(RADIUS Authentication Client MIB)
RFC 2620	(RADIUS Accounting MIB)
RFC 2674	(Dot1p/Q)
RFC 2818	(HTTP over TLS)
RFC 2851	(Internet Addresses MIB)
RFC 2865	(RADIUS Client)
RFC 2866	(RADIUS Accounting)
RFC 2868	(RADIUS Attributes for Tunnel Protocol Support)
RFC 2869	(RADIUS Extensions)
RFC 2869bis	(RADIUS support for EAP)
RFC 2933	(IGMP MIB)
RFC 3164	(The BSD Syslog Protocol)
RFC 3376	(IGMPv3)
RFC 3580	(802.1X RADIUS Usage Guidelines)

A.3 Based specifications and standards

IEEE 802.1 AB	Topology Discovery (LLDP)
IEEE 802.1 af	Power over Ethernet
IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
IEEE 802.1 D-1998	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1 Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)
IEEE 802.1 w.2001	Rapid Reconfiguration (RSTP)
IEEE 802.1 X	Port Authentication
IEEE 802.3 - 2002	Ethernet
IEEE 802.3 ac	VLAN Tagging
IEEE 802.3 ad	Link Aggregation with Static LAG and LACP Support (PowerMICE and MACH 4000)
IEEE 802.3 x	Flow Control

A.4 Copyright of integrated software

A.4.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.4.2 LVL7 Systems, Inc.

(c) Copyright 1999-2006 LVL7 Systems, Inc. All Rights Reserved.

B Readers' comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very good	Good	Satisfactory	Medio-cre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- to

  Hirschmann Automation and Control GmbH
  Department AED
  Stuttgarter Str. 45-51

  72654 Neckartenzlingen

C Index

A
ACA 29, 143
Acceptable Frame Types 91
ACD 146
Address Conflict Detection 146
Advanced 153
AF 101
Alarm 46, 143
Assured Forwarding 101
AutoConfiguration Adapter 143

B
Broadcast 53

C
Cable crossing 25
Class Selector 101
CLI 38, 158
Clock 54
Cold start 24
Command Line Interface 158
Configuring the HIPER-Ring 106
Configuring the MRP-Ring 109
Current VLAN dialog 86

D
Destination port 136
Device status 138
DHCP Option 82 154
DHCP relay agent 154
Diagnose 129
DiffServ 93
DSCP 93

E
EDS 156
EF 101
EtherNet/IP 156
Event Log 130
Expedited Forwarding 101

F
FAQ 173
Filters for MAC addresses 71
Forward Delay 123

G
General 15
Grandmaster 61
GSDML 156

H
Hello Time 123
HIPER-Ring 143
HiVision 7

I
IAONA 145
IGMP Querier 76
IGMP settings 76
IGMP Snooping 76
Independent VLAN 85
Industry Protocols 156
Industry protocols 7
Ingress Filtering 91
IP DSCP mapping 93, 101
IP-DSCP value 94

J
Java Runtime Environment 11
JavaScript 11

L
LLDP 134
Login 12

M
Max Age 123
Media module 143
Multicast 52

N
Network load 132
Network Management Software 7
NTP 51

O
One-Switch coupling 114
Option 82 154

P
Password 12, 38, 39
PHB 101
PLC 156
Port configuration 25, 97
Port mirroring 136
Port priority 97, 98
Port VLAN ID 91
Ports 131
Power over ETHERNET 27
Precedence 101

Precision Time Protocol 54
Priority queue 94
PROFINET 7
PROFINET IO 156
PTP 54

Q
QoS/Priority 93

R
RAM test 148
Rapid Spanning Tree 103, 119
Rapid Spanning Tree dialog 119
Rapid Spanning Tree Port Protocol 125
Rate Limiter 73
Rate Limiter settings 73
Read access 12
Reboot 35
Receiver power status 143
Redundancy 7, 103
Redundancy functions 103
Redundancy Manager 104
Redundant 104
Redundant coupling 103
Reference clock 61
Report 145
Request interval (SNTP) 52
Restart 35
RFC 161
Ring 104
Ring Manager 104
Ring Redundancy 103
Ring Redundancy basic configuration 105
Ring structure 104
Ring/Network Coupling 143
Ring/Network coupling 112
Ringport 106
RM function 104
RMON probe 136
RSTP 103

S
Security 37
Security Data Sheet 145
Self-test 148
Set 13
SFP Module 143
SFP Modules 133
SFP status display 133
Shared VLAN 85
Signal contact 140, 143
SNMP 38
SNTP client 51
SNTP request 51
SNTP server 51
Source port 136
Statistics table 131
Supply voltage 143
Switching 69
Switching Global Dialog 70
Symbol 9
System time 52

T
Technical questions 173
Time 49
Time management 54
Timestamp unit 54
Topology 134
ToS 93
Training courses 173
Trap 46, 143
Trust mode 94
TrustDot1p 94
TrustIpDscp 95
Two-Switch coupling 114
Two-Switch coupling with control line 114
Type of Service 93

U
Universal Time Coordinated 51
Untrusted 94
UTC 51

V
VLAN 83, 108
VLAN and GOOSE Protocol 84
VLAN and redundancy rings 91
VLAN Global dialog 83
VLAN ID 21
VLAN mapping 93, 99
VLAN mode 85
VLAN Port dialog 90
VLAN priority 93, 94
VLAN Static dialog 88
VLAN Transparent Mode 84

W
Web-based Interface 11
Web-based management 12
Website 12
Write access 12

D Further support

Technical questions and training courses

In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office.
You can find the addresses of our distributors on the Internet: www.hirschmann-ac.com.

Our support line is also at your disposal:

- Tel. +49 1805 14-1538
- Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site (www.hirschmann-ac.com) at the end oft the product sites in the FAQ category.
The current training courses to technology and products can be found under http://www.hicomcenter.com.

Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaludation through network planning to project planing.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com.

HIRSCHMANN

A BELDEN BRAND